

(19) 대한민국특허청 (KR)

(12) 공개특허공보 (A)

(51) 。 Int. Cl. 7
G06F 17/00

(11) 공개번호 특2001 - 0082592
(43) 공개일자 2001년08월30일

(21) 출원번호 10 - 2000 - 0079072
(22) 출원일자 2000년12월20일

(30) 우선권주장 1999 - 361225 1999년12월20일 일본 (JP)

(71) 출원인 소니 가부시끼 가이샤
이메이 노부유키
일본국 도쿄도 시나가와쿠 키타시나가와 6쵸메 7반 35고

(72) 발명자 노나카야끼라
일본도쿄도시나가와꾸기따시나가와6쵸메7 - 35소니가부시끼가이샤내
에자끼다다시
일본도쿄도시나가와꾸기따시나가와6쵸메7 - 35소니가부시끼가이샤내

(74) 대리인 장수길
구영창

심사청구 : 없음

(54) 데이터 처리 장치, 데이터 처리 시스템, 및 데이터 처리방법

요약

SAM(Secure Application Module)은 콘텐츠 키 데이터로 암호화된 콘텐츠 데이터, 암호화된 콘텐츠 키 데이터, 및 콘텐츠 데이터의 조작 정책을 지정하는 UCP 데이터가 저장되는 보관 컨테이너를 수신하며, UCP 데이터에 기초한 콘텐츠 데이터의 구매 모드 및 사용 모드를 중 적어도 하나를 결정한다. SAM은 호스트 CPU용 슬레이브로서 작용하며, 또한 호스트 CPU와 공유된 공통 메모리를 구비한다.

대표도
도 1

색인어
콘텐츠, 키, SAM, 컨테이너, 데이터 저장, 암호화

명세서

도면의 간단한 설명

도 1은 본 발명의 제1 실시예에 따른 EMD 시스템의 전체 구성을 도시하는 블록도.

도 2는 본 발명에 사용되는 보관 컨테이너의 개념을 도시한 도면.

도 3a 내지 3c는 콘텐츠 제공자로부터 도 1에 도시된 SAM(Secure Application Module)로 전송된 보관 컨테이너의 포맷을 도시한 도면.

도 4는 도 3a에 도시된 콘텐츠 파일에 포함된 데이터의 상세를 도시한 도면.

도 5는 도 3b에 도시된 키 파일에 포함된 데이터의 상세를 도시한 도면.

도 6은 도 1에 도시된 전자 음악 분배(EMD)와 콘텐츠 제공자 사이의 키 파일의 등록 및 전달을 도시한 도면.

도 7은 콘텐츠 파일에 포함된 헤더 데이터를 도시한 도면.

도 8은 콘텐츠 ID를 도시한 도면.

도 9는 보관 컨테이너의 디렉토리 구조를 도시한 도면.

도 10은 보관 컨테이너의 하이퍼링크 구조를 도시한 도면.

도 11은 제1 실시예에 사용되는 기록 매체(ROM)의 일예를 도시한 도면.

도 12는 제1 실시예에 사용되는 기록 매체(ROM)의 다른 예를 도시한 도면.

도 13은 제1 실시예에 사용되는 기록 매체(ROM)의 다른 예를 도시한 도면.

도 14는 제1 실시예에 사용되는 기록 매체(RAM)의 일예를 도시한 도면.

도 15는 제1 실시예에 사용되는 기록 매체(RAM)의 다른 예를 도시한 도면.

도 16은 제1 실시예에 사용되는 기록 매체(RAM)의 다른 예를 도시한 도면.

도 17, 18 및 19는 콘텐츠 제공자에 의해 보관 컨테이너를 생성하는 처리를 도시한 플로우차트.

도 20은 도 1에 도시된 EMD 서비스 센터의 기능을 도시한 도면.

도 21은 도 1에 도시된 로그 데이터를 도시한 도면.

도 22는 도 1에 도시된 사용자 가정용 네트워크내의 네트워크 디바이스의 구성의 일예를 도시한 블록도.

도 23은 도 22에 도시된 SAM과 호스트 CPU 사이의 관계를 도시한 도면.

도 24는 SAM을 구현하는 소프트웨어 구성을 도시한 도면.

도 25는 호스트 CPU에 출력될 외부 인터럽트를 도시한 도면.

도 26은 호스트 CPU로부터 출력될 외부 인터럽트를 도시한 도면.

도 27은 호스트 CPU로부터 출력될 기능 호출을 도시한 도면.

도 28은 SAM의 CPU의 처리 상태를 도시한 도면.

도 29는 호스트 CPU와 SAM의 메모리 공간을 도시한 도면.

도 30은 도 1에 도시된 사용자 가정용 네트워크내의 SAM의 기능 블록을 도시한 것으로, 콘텐츠 제공자로부터 수신된 보관 컨테이너가 디코딩될 때 데이터 플로우를 도시한 도면.

도 31은 도 22에 도시된 외부 메모리에 저장된 데이터를 도시한 도면.

도 32는 작업 메모리에 저장된 데이터를 도시한 도면.

도 33은 도 1에 도시된 사용자 가정용 네트워크내의 네트워크 디바이스의 구성의 다른 예를 도시한 블록도.

도 34는 도 30에 도시된 저장 유닛에 저장될 데이터를 도시한 도면.

도 35는 EMD 서비스 센터로부터 라이선스 키 데이터를 수신하기 위한 SAM에 의해 수행된 처리를 도시하는 플로우차트.

도 36은 보관 컨테이너를 수신하기 위한 SAM에 의해 수행된 처리를 도시하는 플로우차트.

도 37은 도 1에 도시된 사용자 가정용 네트워크내의 SAM의 기능 블록도로서, 콘텐츠 데이터가 활용되고 구매될 때의 데이터 플로우를 도시한 도면.

도 38은 콘텐츠 데이터의 구매 모드를 결정하기 위한 SAM에 의한 처리를 도시한 플로우차트.

도 39a 내지 39d는 구매 모드가 결정되는 보관 컨테이너를 도시한 도면.

도 40은 콘텐츠 데이터를 재생하기 위해 SAM에 의해서 수행되는 처리를 도시한 플로우차트.

도 41은 구매 모드가 결정되며 도 22에 도시된 네트워크 디바이스의 다운로드 메모리로 다운로드되는 콘텐츠 파일을 시청각(A/V) 기계의 SAM에 전달하는 동작, 및 A/V 기계에서의 콘텐츠 파일을 재구매하는 동작을 도시하는 블록도.

도 42는 도 41에 도시된 수신기 SAM내의 데이터 플로우를 도시한 도면.

도 43은 도 42에 도시된 처리를 도시하는 플로우차트.

도 44a 내지 44d는 도 41에서 전달될 보관 컨테이너의 포맷을 도시한 도면.

도 45는 도 41에 도시된 수신기 SAM에서의 수신된 콘텐츠 파일이 기록 매체(ROM 또는 RAM)으로 기록될 때의 데이터를 도시한 도면.

도 46 및 47은 도 41에 도시된 수신기 SAM에 의한 처리를 도시한 플로우차트.

도 48은 도 1에 도시된 사용자 가정용 네트워크내의 SAM에서의 다양한 구매 모드를 도시한 도면.

도 49는 구매 모드가 결정되지 않은 도 11에 도시된 기록 매체가 사용자 가정용 네트워크로 오프라인 판매될 때, 및 콘텐츠 파일의 구매 모드가 A/V 기계에 의해 결정될 때, A/V 기계내의 데이터 플로우를 도시한 도면.

도 50은 도 49에 도시된 A/V 기계의 SAM내의 데이터 플로우를 도시한 도면.

도 51은 도 49에 도시된 A/V 기계의 SAM에 의해 수행되는 처리를 도시한 플로우차트.

도 52는 사용자 가정용 네트워크내의 A/V 기계의 기록 매체(ROM)로부터, 구매 모드가 결정되지 않은 보관 컨테이너를 판독하며, 보관 컨테이너를 다른 A/V 기계에 전달하며, 이를 기록 매체(RAM)에 기록하는 처리를 도시한 도면.

도 53은 도 52에 도시된 수신기 SAM 내의 데이터 플로우를 도시한 도면.

도 54a 내지 54d는 전송자 SAM으로부터 도 52에 도시된 수신기 SAM으로 전송된 보관 컨테이너의 포맷을 도시한 도면.

도 55 및 56은 전송자 SAM 및 도 52에 도시된 수신기 SAM에 의해 수행되는 처리를 도시한 플로우차트.

도 57은 도 52에 도시된 수신기 SAM내의 데이터 플로우를 도시한 도면.

도 58은 사용자 가정용 네트워크내의 버스를 통해 디바이스의 연결 모델의 예를 도시한 도면.

도 59는 SAM에 의해 생성된 SAM 등록 리스트의 데이터 포맷을 도시한 도면.

도 60은 EMD 서비스 센터에 의해 생성된 공개-키 인증 철회 리스트(public-key certificate revocation list)의 포맷을 도시한 도면.

도 61은 EMD 서비스 센터에 의해 생성된 SAM 등록 리스트의 데이터 포맷을 도시한 도면.

도 62는 SAM의 보안 기능을 도시한 도면.

도 63은 도 1에 도시된 사용자 가정용 네트워크의 네트워크 디바이스에서의 다양한 SAM의 로딩 모델의 일예를 도시한 도면.

도 64는 도 63에 도시된 주변 회로와 다운로드 메모리의 상세한 회로 구성을 도시한 도면.

도 65는 도 63에 도시된 SAM과 호스트 CPU 사이의 관계를 도시한 도면.

도 66은 도 63에 도시된 호스트 CPU, SAM, A/V 압축/압축해제 SAM 및 기록 매체들 사이의 관계를 도시한 도면.

도 67은 도 63에 도시된 호스트 CPU, 매체 구동 SAM, 및 A/V 압축/압축해제 SAM들 사이의 관계를 도시한 도면.

도 68은 정상 처리 SAM의 회로 모듈의 일예를 도시한 도면.

도 69는 도 68에 도시된 회로 모듈로서 구성된 SAM내의 하드웨어 구성의 일예를 도시한 도면.

도 70은 이익 처리 SAM의 어드레스 공간을 도시한 도면.

도 71은 호스트 CPU의 어드레스 공간을 도시한 도면.

도 72는 이익 처리 SAM의 회로 모듈의 다른 예를 도시한 도면.

도 73은 매체 SAM의 회로 모듈을 도시한 도면.

도 74는 ROM이 선적될 때 기록 매체(ROM)의 매체 SAM 내의 저장 데이터를 도시한 도면.

도 75는 등록이 수행된 후 기록 매체(ROM)의 매체 SAM 내의 저장 데이터를 도시한 도면.

도 76은 RAM이 선적될 때 기록 매체(RAM)의 매체 SAM 내의 저장 데이터를 도시한 도면.

도 77은 등록이 수행될 때 저장 매체(RAM)의 매체 SAM 내의 저장 데이터를 도시한 도면.

도 78은 A/V 압축/해제 SAM의 회로 모듈의 예를 도시한 도면.

도 79는 매체 드라이브 SAM의 회로 모듈의 예를 도시한 도면.

도 80은 도 1에 도시된 EMD 시스템의 전체 동작을 도시한 플로우 차트.

도 81은 제1 실시예의 EMD 시스템에서 사용된 안전한 컨테이너용 분배 프로토콜의 예를 도시한 도면.

도 82는 본 발명의 제2 실시예에 따른 EMD 시스템의 전체적인 구성을 도시한 블록도.

도 83은 서비스 제공기 내에 안전한 컨테이너를 생성하기 위한 처리를 도시한 플로우 차트.

도 84a 내지 84d는 서비스 제공기로부터 도 82에 도시된 사용자 홈 네트워크로 보내진 안전한 컨테이너의 포맷을 도시한 도면.

도 85는 도 84a 내지 도 84d에 도시된 안전한 컨테이너내에 저장된 콘텐츠 파일의 송신 포맷을 도시한 도면.

도 86은 도 84a 내지 도 84d에 도시된 안전한 컨테이너내에 저장된 키 파일의 송신 포맷을 도시한 도면.

도 87은 도 82에 도시된 EMD 서비스 센터의 기능을 도시한 도면.

도 88은 도 82에 도시된 네트워크 장치의 기능을 도시한 도면.

도 89는 도 88에 도시된 CA 모듈을 도시한 기능 블록도.

도 90은 도 82에 도시된 SAM을 도시한 기능 블록도로서, 안전한 컨테이너가 수신되고 디코딩될 때 데이터 플로우를 도시한 도면.

도 91은 도 90에 도시된 워크 메모리에 저장될 데이터를 도시한 도면.

도 92는 도 82에 도시된 SAM을 도시한 기능 블록도로서, 콘텐츠의 구입 및 사용 모드가 결정될 때 데이터 흐름을 도시한 도면.

도 93은 도 82에 도시된 SAM에 의해 안전한 컨테이너를 수신하기 위한 처리를 도시한 플로우 차트.

도 94는 구입 모드가 결정되어, 도 82에 도시된 네트워크 장치의 다운로드 메모리로 다운로드된 콘텐츠 파일을 A/V 기기의 SAM으로 전달하는 동작을 도시한 블록도.

도 95는 도 94에 도시된 수신기 SAM 내의 데이터 플로우를 도시한 도면.

도 96은 도 95에 도시된 송신 SAM에 의해 수행된 처리를 도시한 플로우 차트.

도 97a 내지 도 97e는 송신 SAM으로부터 도 94에 도시된 수신기에 전달된 안전한 컨테이너의 포맷을 도시한 도면.

도 98은 도 94에 도시된 수신기 SAM 내의 데이터 플로우를 도시한 도면.

도 99 및 100은 도 94에 도시된 수신기 SAM에 의해 수행된 처리를 도시한 플로우 차트.

도 101은 도 82에 도시된 사용자 홈 네트워크 내의 SAM의 접속 모델의 예를 도시한 도면.

도 102 및 103은 도 82에 도시된 EMD 시스템의 전체적인 동작을 도시한 플로우 차트.

도 104는 도 82에 도시된 EMD 시스템의 서비스 모델의 예를 도시한 도면.

도 105는 도 82에 도시된 EMD 시스템에서 사용된 안전한 컨테이너용 분배 프로토콜을 도시한 도면.

도 106은 종래의 EMD 시스템을 도시한 블록도.

< 도면의 주요 부분에 대한 부호의 설명 >

100 : EMD 시스템

101 : 콘텐츠 제공자

102 : EMD 서비스 센터

103 : 사용자 홈 네트워크

106 ; UCP 데이터

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 제공된 콘텐츠 데이터에 대한 처리를 수행하기 위한 데이터 처리 장치 및 시스템과, 이런 장치 및 시스템에 대한 데이터 처리 방법에 관한 것이다.

암호화된 콘텐츠 데이터를 선정된 계약을 행한 사용자의 데이터 처리 장치로 분배하며, 데이터 처리 장치가 콘텐츠 데이터를 디코딩하며 판독 및 기록가능하게 하기 위한 데이터 제공 시스템이 이용가능하다. 그런 데이터 제공 시스템 중 하나의 타입은 음악 데이터를 분배하기 위한 종래의 전자 음악 분배(EMD) 시스템이다.

도 106은 종래의 EMD 시스템(700)을 도시하는 개요도이다. EMD 시스템(700)에서, 콘텐츠 제공자(701a 및 701b)는 상호 인증을 수행한 후 얻어진 세션 키 데이터를 사용함에 의해 콘텐츠 데이터(704a, 704b 및 704c)와 저작권 정보(705a, 705b 및 705c)를 암호화하고, 그 후 암호화된 데이터를 서비스 제공자(710)에 온라인 또는 오프라인으로 제공한다. 저작권 정보(705a, 705b 및 705c)는 적절 카피 관리 시스템 정보(SCMS), 저작권 정보를 콘텐츠 데이터에 내장시키기 위한 디지털 워터마크(watermark), 저작권 정보를 서비스 제공자(710)의 전송 프로토콜에 내장시키기 위한 정보를 포함할 수 있다.

서비스 제공자(710)는 세션 키 데이터의 사용에 의하여 수신된 콘텐츠 데이터(704a, 704b 및 704c)와 저작권 정보(705a, 705b 및 705c)를 디코딩한다.

서비스 제공자(710)는 저작권 정보(705a, 705b 및 705c)를 콘텐츠 데이터(707a, 707b 및 707c)를 생성하기 위하여 온라인 또는 오프라인으로 수신되는 디코딩된 콘텐츠 데이터(704a, 704b 및 704c)로 내장시킨다. 이런 경우에, 저작권 정보(705a, 705b 및 705c)의 일부로서, 서비스 제공자(710)는 선정된 주파수 영역을 변경함에 의해 디지털 워터마크 정보를 콘텐츠 데이터(704a, 704b 및 704c)로 내장시키며, SCMS 정보를, 콘텐츠 데이터(704a, 704b 및 704c)를 사용자에게 전송하는데 사용되는 네트워크 프로토콜로 내장시킨다.

서비스 제공자(710)는 또한 키 데이터베이스(706)로부터 판독된 콘텐츠 키 데이터(Kca, Kcb 및 Kcc)를 사용함에 의해 콘텐츠 데이터(707a, 707b 및 707c)를 암호화한다. 연속해서, 서비스 제공자(710)는 상호 인증을 수행한 후 얻어진 세션 키 데이터를 사용함에 의해 암호화 콘텐츠 데이터(707a, 707b 및 707c)를 저장하는 보관 컨테이너(722)를 암호화하고, 암호화된 보관 컨테이너(722)를 사용자의 단자 디바이스(709)에 저장된 조건 액세스(CA) 모듈(711)에 전송한다.

CA 모듈(711)은 세션 키 데이터를 사용함에 의해 보관 컨테이너(722)를 디코딩한다. CA 모듈(711)은 전자 해결 시스템 또는 CA와 같은 계정 기능을 사용함에 의해 서비스 제공자(710)의 키 데이터베이스(706)로부터의 콘텐츠 키 데이터(Kca, Kcb 및 KCC)를 또한 수신하며, 이를 세션 키 데이터를 사용함에 의해 디코딩한다. 이는 콘텐츠 키 데이터(Kca, Kcb 및 KCC)를 각각 사용함에 의해 단자 디바이스(709)가 콘텐츠 키 데이터(Kca, Kcb 및 KCC)를 디코딩 가능하게 한다.

CA 모듈(711)은 계정 정보(721)를 발생시키기 위하여 각각의 콘텐츠에 대한 계정 처리를 수행하며, 이를 세션 키 데이터를 사용함에 의해 암호화하며, 이를 서비스 제공자(710)의 정상 처리 모듈(720)로 전송한다.

이런 경우, CA 모듈(711)은 서비스 제공자(710)에 의해 제공된 서비스에 관한 아이템, 달리 말하자면 사용자 계약(제 계약) 정보와 같은 서비스 제공자(710)에 의해 관리되는 아이템에 대한 처리, 예컨대 네트워크를 사용함에 의해 부과되는 대당 기본 요금의 수집에 대한 처리, 네트워크의 물리층의 보안을 보장을 수행한다.

CA 모듈(711)로부터 계정 정보를 수신할 때, 서비스 제공자(710)는 서비스 제공자(710)와 콘텐츠 제공자(701a, 701b, 701c)간에 이익을 분배한다. 이런 경우, 이익은 예컨대, JASRAC(Japanese Society for Rights of Authors, Composers and Publishers)인 중개자를 통해 서비스 제공자(710)로부터 콘텐츠 제공자(701a, 701b 및 701c)로 분배된다. JASRAC는 또한 콘텐츠 제공자(701a, 701b 및 701c)의 이익을 저작권 홀더, 예술가, 작곡가, 극작가, 및 콘텐츠 데이터의 제작사 등에 분배한다.

예컨대 RAM과 같은 기록 매체(723) 상에서 콘텐츠 키 데이터(Kca, Kcb 및 KCC)로 디코딩된 콘텐츠 데이터(707a, 707b 및 707c)를 기록할 때, 단자 디바이스(709)는 저작권 정보(705a, 705b 및 705c)의 SCMS 비트를 중복기재함에 의해 카피 제어를 수행한다. 즉, 사용자는 콘텐츠 데이터(707a, 707b 및 707c)로 내장된 SCMS 비트에 기초하여 카피 제어를 수행하여 저작권 보호를 구현한다.

SCMS는 콘텐츠 데이터의 복사 동작, 예컨대 2 이상의 발생(복사 무료)하는 것을 방지하나, 제한되지 않는 하나의 발생 복사(한번의 카피)를 허용하며, 따라서 저작권 보호에 불충분하게 된다.

상술한 EMD 시스템(700)에서는 콘텐츠 제공자(701)가 암호화되지 않은 콘텐츠 데이터를 기술적으로 자유롭게 조작할 수 있으며 콘텐츠 제공자(701a, 701b 및 701c)가 불공정하게 이용할 수 있는 서비스 제공자(710)의 역할을 모니터링할 필요가 있다.

부가적으로, EMD 시스템(700)에서는 서비스 제공자(710)로부터 분배된 콘텐츠 데이터터를 창작하며 이를 다른 단자 디바이스에 재분배하여, 콘텐츠 제공자(701a, 701b 및 701c)의 이익을 불법적으로 이용하게 되는 것과 같은 사용자의 단자 디바이스(709)의 불법적인 액션을 제한하는 것이 어렵게 된다.

발명이 이루고자 하는 기술적 과제

따라서, 상술한 문제점을 해결하기 위하여, 본 발명의 일목적은 콘텐츠 제공자와 같은 콘텐츠 권리 보유자의 이익을 적절히 보호할 수 있는 데이터 처리 장치, 데이터 처리 시스템 및 데이터 처리 방법을 제공하는 것이다.

본 발명의 다른 목적은 콘텐츠 제공자와 같은 콘텐츠 권리 보유자의 이익을 보호하기 위한 로드를 감소시키기 위한 데이터 처리 장치, 데이터 처리 시스템 및 데이터 처리 방법을 제공하는 것이다.

발명의 구성 및 작용

상기 목적을 달성하기 위하여, 본 발명의 일면에 따르면, 사용 제한 정책 데이터에 근거하여 콘텐츠 키 데이터로 암호화된 콘텐츠 데이터의 정상 처리를 실시하고, 암호화된 콘텐츠 키 데이터를 해독하기 위한 데이터 처리 장치에 있어서, 제1 버스; 상기 제1 버스에 접속되고, 상기 사용 제한 정책 데이터에 근거하여 상기 콘텐츠 데이터의 정상 처리를 실시하는 연산 처리 회로; 상기 제1 버스에 접속된 기억 회로; 제2 버스; 상기 제1 버스와 상기 제2 버스 사이에 배치된 제1 인터페이스 회로; 상기 제2 버스에 접속되어 상기 콘텐츠 키 데이터를 해독하는 암호 처리 회로; 및 상기 제2 버스에 접속된 외부 버스 인터페이스 회로를 조작 방지 회로(tamper-resistant circuit) 모듈내에 포함하는 것을 특징으로 하는 데이터 처리 장치가 제공된다.

상술한 데이터 처리 장치에 따르면, 콘텐츠 데이터, 대응하는 콘텐츠 키 데이터 및 대응하는 UCP 데이터가 분배되고, 또한 콘텐츠 키 데이터를 해독하기 위한 라이선스 키 데이터가 분배된다. 라이선스 키 데이터는 예컨대 상술한 저장 회로에 저장된다.

이후, 외부 버스 인터페이스 회로를 통해 외부 연산 처리 장치로부터 정상 처리를 수행하기 위해 지시에 응답하여, UCP 데이터를 기초로 한 콘텐츠 데이터의 정상 처리는 상술한 연산 처리 회로에서 실행된다. 그 후, 콘텐츠 키 데이터는 저장 회로로부터 판독된 라이선스 키 데이터를 사용함에 의해 연산 처리 회로에서 해독된다.

상술한 데이터 처리 장치는 다른 디코딩 장치로 상호 인증을 수행하고, 상호 인증에 의해 얻어진 세션 키 데이터를 사용함에 의해 해독된 콘텐츠 키 데이터 및 콘텐츠 데이터를 암호화한다.

상술한 데이터 처리 장치는 조작 방지 회로 모듈내에서 제2 인터페이스 회로를 포함한다. 제1 버스는 연산 처리 회로 및 저장 회로에 연결된 제3 버스 및 제1 인터페이스 회로에 연결된 제4 버스를 포함하고, 제2 인터페이스 회로는 제3 버스와 제4 버스간에 삽입된다.

상술한 데이터 처리 장치는, 상기 조작 방지 회로 모듈내에 제5 버스; 상기 제5 버스에 접속되어, 기록 매체와 집적회로 카드중 하나에 로드되는 인증 기능을 갖춘 데이터 처리 회로와의 통신을 실시하는 제3 인터페이스 회로; 및 상기 제4 버스와 상기 제5 버스 사이에 배치된 제4 인터페이스 회로를 더 포함한다.

상술한 데이터 처리 장치에서는 상기 암호 처리 회로가 공개 키(public-key) 암호 회로 및 공통 키(common-key) 암호 회로를 포함한다.

상술한 데이터 처리 장치에서, 상기 기억 회로는 상기 데이터 처리 장치의 전용 키(private key) 데이터 및 제2 데이터 처리 장치의 공개 키 데이터를 기억하고;

상기 공개 키 암호 화서는 상기 콘텐츠 데이터, 상기 콘텐츠 키 데이터, 상기 사용 제한 정책 데이터의 완전성(integrity)을 검증하는 서명 데이터의 완전성을 대응하는 공개 키 데이터를 사용하여 검증하며, 상기 콘텐츠 데이터, 상기 콘텐츠 키 데이터, 상기 사용 제한 정책 데이터를 기록 매체에 기록하거나 이들을 상기 제2 데이터 처리 장치로 전송할 때, 상기 공개 키 암호 화서는 상기 콘텐츠 데이터, 상기 콘텐츠 키 데이터, 상기 사용 제한 정책 데이터의 완전성을 검증하는 서명 데이터를 상기 전용 키 데이터를 사용하여 생성하며;

상기 공통 키 암호 화서는 상기 콘텐츠 키 데이터를 해독하고, 상기 콘텐츠 데이터, 상기 콘텐츠 키 데이터, 상기 사용 제한 정책 데이터를 온라인으로 상기 제2 데이터 처리 장치로 전송할 때, 상기 공통 키 암호 화서는 상기 제2 데이터 처리 장치와의 상호 인증을 실시하여 구해진 세션 키 데이터를 사용하여 상기 콘텐츠 데이터, 상기 콘텐츠 키 데이터, 상기 사용 제한 정책 데이터를 암호화하고 해독한다.

상술한 데이터 처리 장치는 상기 조작 방지 회로 모듈내에 상기 콘텐츠 데이터, 상기 콘텐츠 키 데이터, 상기 사용 제한 정책 데이터의 해쉬값을 발생시키기 위한 해쉬값 발생 회로를 더 포함한다. 상기 공개 키 암호 화서는 상기 해쉬값을 이용하여 상기 서명 데이터의 완전성을 검증하고 서명 데이터를 생성한다.

상술한 데이터 처리 장치는 상기 조작 방지 회로 모듈내에 난수 발생 회로를 더 포함한다. 상기 난수 발생 회로는 상기 제2 버스에 접속되어, 상기 콘텐츠 데이터, 상기 콘텐츠 키 데이터, 상기 사용 제한 정책 데이터를 온라인으로 상기 제2 데이터 처리 장치로 전송할 때 상기 제2 데이터 처리 장치와의 상호 인증을 실시하기 위한 난수를 발생한다.

상술한 데이터 처리 장치에서 상기 외부 버스 인터페이스 회로는 상기 콘텐츠 데이터, 상기 콘텐츠 키 데이터, 상기 사용 제한 정책 데이터중 적어도 하나를 기억하는 외부 기억 회로에 접속될 수 있다.

데이터 처리 장치는 상기 연산 처리 회로로부터의 커맨드에 따라 상기 기억 회로로의 액세스 및 상기 외부 버스 인터페이스 회로를 경유한 상기 외부 기억 회로로의 액세스를 제어하기 위한 기억 회로 제어 회로를 더 포함한다.

상술한 데이터 처리 장치에서, 상기 외부 버스 인터페이스 회로는 상기 데이터 처리 장치가 로드되는 시스템을 중앙 제어하기 위한 호스트 연산 처리 장치에 접속된다.

상술한 데이터 처리 장치는 상기 기억 회로의 어드레스 공간 및 상기 외부 기억 회로의 어드레스 공간을 관리하기 위한 기억부 관리 회로를 더 포함한다.

상술한 데이터 처리 장치에서, 상기 연산 처리 회로는 상기 사용 제한 정책 데이터에 의해 표시되는 처리 정책에 근거하여 콘텐츠 데이터의 구입 모드 및 사용 모드중 적어도 하나를 판정하고, 판정된 모드의 결과를 표시하는 로그 데이터를 생성한다.

상술한 데이터 처리 장치에서, 구입 모드 판정 후에, 상기 연산 처리 회로는 판정된 구입 모드에 따라 사용 제한 상태 데이터를 생성하고, 상기 사용 제한 상태 데이터에 근거하여 콘텐츠 데이터의 사용을 제한한다.

상술한 데이터 처리 장치에서, 구입 모드로 판정된 콘텐츠 데이터를 기록 매체에 기록할 때, 상기 공통 키 암호 화서는 상기 기록 매체에 대응하는 매체 키 데이터를 사용하여 상기 콘텐츠 키 데이터 및 상기 사용 제한 상태 데이터를 암호화한다.

상술한 데이터 처리 장치에서, 상기 콘텐츠 키 데이터가 유효 기간을 가진 라이선스 키 데이터로 암호화될 때, 상기 기억 회로는 상기 라이선스 키 데이터를 기억하고, 상기 데이터 처리 장치는 실시간을 발생하기 위한 실시간 클럭을 더 포함하며, 상기 연산 처리 회로는 상기 실시간 클럭에 의해 표시된 실시간에 근거하여 상기 기억 회로로부터 유효 라이선스 키 데이터를 판독하고, 상기 공통 키 암호 화서는 판독된 라이선스 키 데이터를 사용하여 콘텐츠 키 데이터를 해독한다.

데이터 처리 장치에서, 상기 기억 회로는 블록 단위로 데이터를 기입 및 소거하며, 상기 데이터 처리 장치는 상기 연산 처리 회로의 제어하에 데이터를 상기 기억 회로에 블록 단위로 기입 및 소거하는 것을 제어하기 위한 기입 - 록 제어 회로를 상기 조작 방지 회로 모듈내에 포함한다.

본 발명의 다른 면에 따르면, 사용 제한 정책 데이터에 근거하여 콘텐츠 키 데이터로 암호화된 콘텐츠 데이터의 정상 처리를 실시하고, 암호화된 콘텐츠 키 데이터를 해독하기 위한 데이터 처리 장치가 제공된다. 데이터 처리 장치는 제1 버스; 상기 제1 버스에 접속되고, 상기 사용 제한 정책 데이터에 근거하여 상기 콘텐츠 데이터의 정상 처리를 실시하는 연산 처리 회로; 상기 제1 버스에 접속된 기억 회로; 제2 버스; 상기 제1 버스와 상기 제2 버스 사이에 배치된 인터페이스 회로; 상기 제2 버스에 접속되어 상기 콘텐츠를 키 데이터를 해독하는 암호 처리 회로; 및 상기 제2 버스에 접속된 외부 버스 인터페이스 회로를 조작 방지 회로 모듈내에 포함하며, 상기 외부 버스 인터페이스 회로를 거쳐 외부 회로로부터 인터럽트를 수신하면, 상기 연산 처리 회로는 상기 인터럽트에 의해 지정된 처리를 실시하도록 상기 외부 회로에 대한 슬레이브가 되어, 그 연산의 결과를 상기 외부 회로에 보고한다.

상술한 데이터 처리 장치에서, 상기 연산 처리 회로는 상기 외부 회로로 인터럽트를 출력함으로써 처리의 결과를 보고한다.

상술한 데이터 처리 장치에서, 상기 외부 버스 인터페이스는 상기 연산 처리 회로 및 상기 외부 회로를 위한 공통 메모리를 포함하고, 상기 연산 처리 회로는 처리의 결과를 상기 공통 메모리에 기입하며, 상기 외부 회로는 폴링을 통해 처리의 결과를 구한다.

상술한 데이터 처리 장치에서, 상기 외부 버스 인터페이스는, 상기 연산 처리 회로에 상기 외부 회로로부터 요청된 처리의 실행 상태를 표시하고, 상기 연산 처리 회로에 의해 설정되며 상기 외부 회로에 의해 판독되는 플래그를 포함하는 제1 상태 레지스터; 상기 외부 회로가 상기 연산 처리 회로에 처리를 실시하도록 요청하였는지 여부를 표시하고, 상기 외부 회로에 의해 설정되며 상기 연산 처리 회로에 의해 판독되는 플래그를 포함하는 제2 상태 레지스터; 및 처리의 결과를 기억하기 위한 상기 공통 메모리를 포함한다.

데이터 처리 장치에서, 상기 기억 회로는 인터럽트에 의해 지정된 처리를 기술한 인터럽트 프로그램을 기억하고, 상기 연산 처리 회로는 상기 기억 회로로부터 판독된 인터럽트 프로그램을 실행하여 처리를 실시한다.

데이터 처리 장치에서, 상기 기억 회로는 복수의 상기 인터럽트 프로그램과, 인터럽트 프로그램을 실행할 때 판독될 복수의 서브 - 루틴을 기억하고, 상기 연산 처리 회로는 상기 기억 회로로부터 판독된 인터럽트 프로그램을 실행할 때 상기 기억 회로로부터 서브 - 루틴을 적절히 판독하고 실행한다.

본 발명의 다른 면에 따르면, 선정된 프로그램을 실행하고, 마스터로서 작용하여 선정된 조건에 따라 인터럽트를 출력하는 연산 처리 장치와; 상기 연산 처리 장치에 대한 슬레이브로서 작용하여 상기 연산 처리 장치로부터의 인터럽트에 응답하여 선정된 처리를 실시하고, 처리의 결과를 상기 연산 처리 장치에 보고하는 데이터 처리 장치를 포함하며, 상기 데이터 처리 장치는, 사용 제한 정책 데이터에 의해 표시되는 처리 정책에 근거하여 콘텐츠 데이터의 구입 모드 및 사용 모드중 적어도 하나를 판정하는 판정 수단; 판정된 모드의 결과를 표시하는 로그 데이터를 발생시키는 로그 데이터 발생 수단; 및 콘텐츠 키 데이터를 해독하는 해독 수단을 조작 방지 회로 모듈내에 포함하는 데이터 처리 시스템이 제공된다.

상술한 데이터 처리 시스템에서, 인터럽트 타입을 표시하는 인터럽트를 수신하면, 상기 연산 처리 장치는 인터럽트 타입에 대응하는 인터럽트 루틴을 실행하라는 명령을 표시하는 인터럽트를 상기 데이터 처리 장치에 출력하고, 상기 데이터 처리 장치는 상기 연산 처리 장치로부터 수신된 인터럽트의 인터럽트 타입에 대응하는 인터럽트 루틴을 실행한다.

상술한 데이터 처리 시스템에서, 상기 데이터 처리 장치는 상기 연산 처리 장치로 인터럽트를 출력함으로써 처리의 결과를 보고한다.

상술한 데이터 처리 시스템에서, 상기 데이터 처리 장치는 상기 데이터 처리 장치 및 상기 연산 처리 장치에 의해 액세스 가능한 공통 메모리를 포함하고, 상기 연산 처리 장치는 폴링을 통해 상기 공통 메모리에 액세스함으로써 처리의 결과를 구한다.

상술한 데이터 처리 시스템에서, 상기 데이터 처리 장치는 상기 연산 처리 장치로부터 요청된 처리의 실행 상태를 표시하고, 상기 연산 처리 장치에 의해 판독되는 플래그를 포함하는 제1 상태 레지스터; 상기 연산 처리 장치가 상기 데이터 처리 장치에 인터럽트에 의한 처리를 실시하도록 요청하였는지 여부를 표시하고, 상기 연산 처리 장치에 의해 설정되는 플래그를 포함하는 제2 상태 레지스터; 및 처리의 결과를 기억하기 위한 상기 공통 메모리를 포함한다.

상술한 데이터 처리 시스템에서, 상기 연산 처리 장치와 상기 데이터 처리 장치를 접속하기 위한 버스를 더 포함한다.

상술한 데이터 처리 시스템에서, 상기 데이터 처리 장치는 초기 프로그램 및 인터럽트 루틴중 하나의 실행을 완료한 후에 저전력 상태로 들어간다.

상술한 데이터 처리 시스템에서, 상기 연산 처리 장치로부터 수신된 인터럽트에 근거하여, 상기 데이터 처리 장치는 콘텐츠 데이터의 구입 모드 및 사용 모드중 하나를 판정하는 처리와, 콘텐츠 데이터를 제공하는 처리와, 인증 기관(certifying authority)으로부터 데이터를 다운로드하는 처리중 적어도 하나에 따라 인터럽트 루틴을 실행한다.

상술한 데이터 처리 시스템에서, 상기 연산 처리 장치는 선정된 사용자 프로그램을 실행한다.

본 발명의 다른 면에 따르면, 데이터 처리 장치에 의해 제공되는 콘텐츠 데이터가 데이터 분배 장치로부터 수신되고 관리 장치에 의해 관리되는 데이터 처리 시스템이 제공된다. 데이터 처리 시스템은, 콘텐츠 키 데이터로 암호화된 콘텐츠 데이터와, 암호화된 콘텐츠 키 데이터와, 콘텐츠 데이터의 처리 정책을 표시하는 사용 제한 정책 데이터와, 상기 데이터 분배 장치에 의해 결정된 콘텐츠 데이터에 대한 가격 데이터가 기억되어 있는 모듈을 상기 데이터 분배 장치로부터 수신하고, 상기 수신된 모듈을 공통 키 데이터를 사용하여 해독하며, 상기 데이터 분배 장치에 의한 모듈의 분배 서비스에 대한 아카운팅 처리를 실시하는 제1 처리 모듈; 선정된 프로그램을 실행하고, 마스터로서 작용하여 선정된 조건에 따라 인터럽트를 출력하는 연산 처리 장치; 및 상기 연산 처리 장치에 대한 슬레이브로서 작용하여 상기 연산 처리 장치로부터의 인터럽트에 응답하여 선정된 처리를 실시하고, 처리의 결과를 상기 연산 처리 장치에 보고하는 데이터 처리 장치를 포함하며, 상기 데이터 처리 장치는, 수신된 모듈에 기억되어 있는 사용 제한 정책 데이터에 의해 표시되는 처리 정책에 근거하여 콘텐츠 데이터의 구입 모드 및 사용 모드중 적어도 하나를 판정하는 판정 수단; 판정된 모드의 결과를 표시하는 로그 데이터를 발생시키는 로그 데이터 발생 수단; 콘텐츠 데이터의 구입 모드가 판정될 때 상기 관리 장치로 상기 가격 데이터 및 로그 데이터를 출력하는 출력 수단; 및 콘텐츠 키 데이터를 해독하는 해독 수단을 조작 방지 회로 모듈내에 포함한다.

본 발명의 다른 면에 따르면, 선정된 프로그램을 실행하고, 마스터로서 작용하여 선정된 조건에 따라 인터럽트를 출력하는 연산 처리 장치; 상기 연산 처리 장치에 대한 슬레이브로서 작용하여 상기 연산 처리 장치로부터의 인터럽트에 응답하여 콘텐츠 키 데이터로 암호화된 콘텐츠 데이터의 정상 처리를 실시하고, 처리의 결과를 상기 연산 처리 장치에 보고하는 제1 조작 방지 데이터 처리 장치; 및 상기 제1 조작 방지 데이터 처리 장치와의 상호 인증을 실시하여 구현된 콘텐츠 키 데이터를 사용하여 콘텐츠 데이터를 해독하고, 상기 연산 처리 장치 또는 상기 제1 조작 방지 데이터 처리 장치에 대한 슬레이브로서 작용하여 상기 연산 처리 장치 또는 상기 제1 조작 방지 데이터 처리 장치로부터의 인터럽트에 응답하여 콘텐츠 데이터를 압축 또는 압축해제하는 제2 조작 방지 데이터 처리 장치를 포함하는 데이터 처리 시스템이 제공된다.

상술한 데이터 처리 시스템은 상기 연산 처리 장치와, 상기 제1 조작 방지 데이터 처리 장치와, 상기 제2 조작 방지 데이터 처리 장치를 접속하기 위한 버스를 더 포함한다.

본 발명의 다른 면에 따르면, 선정된 프로그램을 실행하고, 마스터로서 작용하여 선정된 조건에 따라 인터럽트를 출력하는 연산 처리 장치; 상기 연산 처리 장치에 대한 슬레이브로서 작용하여 상기 연산 처리 장치로부터의 인터럽트에 응답하여 콘텐츠 키 데이터로 암호화된 콘텐츠 데이터의 정상 처리를 실시하고, 처리의 결과를 상기 연산 처리 장치에 보고하는 제1 조작 방지 데이터 처리 장치; 및 상기 연산 처리 장치와의 상호 인증을 실시하고, 상기 연산 처리 장치로부터의 인터럽트 출력에 응답하여 콘텐츠 데이터를 기록 매체로부터 판독하고 기록 매체에 기입하는 제2 조작 방지 데이터 처리 장치를 포함하는 데이터 처리 시스템이 제공된다.

상술한 데이터 처리 시스템에서, 상기 제2 조작 방지 처리 장치는 상기 기록 매체에 대응하는 매체 키 데이터를 사용하여 콘텐츠 데이터를 해독 및 암호화한다.

상술한 데이터 처리 시스템에서, 상기 기록 매체에 상호 인증 기능을 갖는 처리 회로가 제공되는 경우, 상기 제2 조작 방지 처리 장치는 상기 처리 회로와의 상호 인증을 실시한다.

본 발명의 다른 면에 따르면, 선정된 프로그램을 실행하고, 마스터로서 작용하여 선정된 조건에 따라 인터럽트를 출력하는 연산 처리 장치; 상기 연산 처리 장치와의 상호 인증을 실시하고, 상기 연산 처리 장치로부터의 인터럽트 출력에 응답하여 콘텐츠 데이터를 기록 매체로부터 판독하고 기록 매체에 기입하는 제1 조작 방지 데이터 처리 장치; 및 콘텐츠 키 데이터를 사용하여 콘텐츠 데이터를 해독하고, 상기 연산 처리 장치에 대한 슬레이브로서 작용하여 상기 연산 처리 장치로부터의 인터럽트에 응답하여 콘텐츠 데이터를 압축 또는 압축해제하는 제2 조작 방지 데이터 처리 장치를 포함하는 데이터 처리 시스템이 제공된다.

상술한 데이터 처리 시스템은 상기 제1 조작 방지 데이터 처리 장치에 의해 상기 기록 매체로부터 판독된 콘텐츠 데이터를 일시적으로 기억하고, 기억된 콘텐츠 데이터를 상기 제2 조작 방지 데이터 처리 장치로 출력하는 기억 회로를 더 포함한다.

상술한 데이터 처리 시스템에서, 상기 기억 회로는 진동 방지 기억 회로의 기억 영역 부분을 이용한다.

상술한 데이터 처리 시스템은 상기 연산 처리 장치에 대한 슬레이브로서 작용하여 상기 연산 처리 장치로부터의 인터럽트에 응답하여 콘텐츠 키 데이터로 암호화된 콘텐츠 데이터의 정상 처리를 실시하고, 처리의 결과를 상기 연산 처리 장치에 보고하는 제3 조작 방지 데이터 처리 장치를 더 포함한다.

본 발명의 다른 면에 따르면, 연산 처리 장치와 데이터 처리 장치를 사용하여 데이터를 처리하는 방법이 제공된다. 데이터 처리 방법은, 상기 연산 처리 장치에서, 선정된 프로그램을 실행하고, 마스터로서 작용하여 선정된 조건에 따라 인터럽트를 출력하는 단계와; 상기 데이터 처리 장치에서, 상기 연산 처리 장치에 대한 슬레이브로서 작용하여 상기 연산 처리 장치로부터의 인터럽트에 응답하여, 조작 방지 회로 모듈내에서, 사용 제한 정책 데이터의 처리 정책에 근거하여 콘텐츠 데이터의 구입 모드 및 사용 모드중 적어도 하나를 판정하고, 판정된 모드의 결과를 표시하는 로그 데이터를 생성하며, 콘텐츠 키 데이터를 해독하는 단계를 포함한다.

본 발명의 다른 면에 따르면, 연산 처리 장치, 제1 데이터 처리 장치, 및 제2 데이터 처리 장치를 사용하는 데이터 처리 방법이 제공된다. 데이터 처리 방법은, 상기 연산 처리 장치에서, 선정된 프로그램을 실행하며, 마스터로서 작용함에 의해 선정된 조건에 따라 인터럽트를 출력하는 단계; 상기 제1 데이터 처리 장치에서, 슬레이브로서 작용함에 의해 상기

연산 처리 장치로부터 상기 인터럽트에 응답하여 조작 방지 모듈내의 콘텐츠 키 데이터로 암호화된 콘텐츠 데이터의 정상 처리를 수행하며, 상기 처리의 결과를 상기 연산 처리 장치에 리포트하는 단계, 및 상기 제2 데이터 처리 장치에서, 상기 제1 데이터 처리 장치내에서 상호 인증을 수행함에 의해 얻어진 상기 콘텐츠 키 데이터를 사용함에 의해 상기 콘텐츠 데이터를 해독하며, 상기 연산 처리 장치 또는 상기 제1 데이터 처리 장치를 슬레이브로서 작용함에 의해 상기 연산 처리 장치 또는 상기 제1 데이터 처리 장치로부터의 인터럽트에 응답하여 조작 방지 모듈내의 콘텐츠 데이터를 압축 또는 압축해제하는 단계를 포함한다.

본 발명의 다른 면에 따르면, 연산 처리 장치, 제1 데이터 처리 장치 및 제2 데이터 처리 장치를 사용하는 데이터 처리 방법이 제공된다. 데이터 처리 방법은,

상기 연산 처리 장치에서, 선정된 프로그램을 실행하며, 마스터로서 작용함에 의해 선정된 조건에 따라 인터럽트를 출력하는 단계; 상기 제1 데이터 처리 장치에서, 슬레이브로서 작용함에 의해 상기 연산 처리 장치로부터 상기 인터럽트에 응답하여 조작 방지 모듈내의 콘텐츠 키 데이터로 암호화된 콘텐츠 데이터의 정상 처리를 수행하며, 상기 처리의 결과를 상기 연산 처리 장치에 리포트하는 단계, 및 상기 제2 데이터 처리 장치에서, 상기 연산 처리 장치로 상호 인증을 수행하며, 상기 연산 처리 장치로부터의 상기 인터럽트에 응답하여 조작 방지 모듈내의 기록 매체로/로부터 상기 콘텐츠 데이터를 판독 및 기록하는 단계를 포함한다.

본 발명의 다른 면에 따르면, 연산 처리 장치, 제1 데이터 처리 장치, 및 제2 데이터 처리 장치를 사용하는 데이터 처리 방법이 제공된다. 데이터 처리 방법은, 상기 연산 처리 장치에서, 선정된 프로그램을 실행하며, 마스터로서 작용함에 의해 선정된 조건에 따라 인터럽트를 출력하는 단계; 상기 제1 데이터 처리 장치에서, 상기 연산 처리 장치로 상호 인증을 수행하며, 상기 연산 처리 장치로부터의 인터럽트에 응답하여 조작 방지 모듈내의 기록 매체로/로부터 콘텐츠 데이터를 판독 및 기록하는 단계; 및 상기 제2 데이터 처리 장치에서, 콘텐츠 키 데이터를 사용함에 의해 상기 콘텐츠 데이터를 해독하며, 상기 연산 처리 장치를 슬레이브로서 작용함에 의해 상기 연산 처리 장치로부터의 인터럽트에 응답하여 조작 방지 모듈내의 상기 콘텐츠 데이터를 압축 또는 압축해제하는 단계를 포함한다.

본 발명의 실시예에 따른 전자 음악 분배(EMD) 시스템이 먼저 아래에 설명된다.

제1 실시예

도 1은 본 발명의 실시예에 따라 구성된 EMD 시스템(100)을 도시한 블록도이다.

본 실시예에서, 사용자에게 분배될 "콘텐츠 데이터"는 예로서 음악 데이터를 들어 아래에 설명되는, 의미있는 정보를 갖는 디지털 데이터이다.

EMD 시스템(100)은 도 1에 도시한 바와 같이, 콘텐츠 제공기(101), EMD 서비스 센터(정보 분류 정리국은 이후 "ESC"로 간단히 함)(102), 및 사용자 홈 네트워크(103)를 포함한다.

콘텐츠 제공기(101), EMD 서비스 센터(102), 및 안전 응용 모듈(SAM)(105, 내지 105₄)는 각각 본 발명의 데이터 제공 장치, 데이터 관리 장치, 및 데이터 처리 장치에 대응한다.

EMD 시스템(100)의 개관이 먼저 논의된다. EMD 시스템(100)은 매우 신뢰할 수 있는 공인 기구인 EMD 서비스 센터(102)에, 제공될 콘텐츠 데이터 C를 암호화하기 위해 사용되는 콘텐츠 키 데이터 Kc, 예를 들어, 콘텐츠 데이터 C의 라이선스 계약 조건을 표시하는 UCP(UCP) 데이터(106), 및 디지털 워터마크 정보의 콘텐츠 및 디지털 워터마크가 매립되는 위치를 표시하는 디지털 - 워터마크 정보 제어 데이터를 보낸다.

EMD 서비스 센터(102)는 콘텐츠 제공기(101)로부터 수신된 콘텐츠 키 데이터 Kc, UCP 데이터(106), 및 디지털 - 워터마크 정보 제어 데이터를 등록(인증 또는 공인)한다.

EMD 서비스 센터(102)는 또한 대응하는 주기의 라이선스 키 데이터 KD₁ 내지 KD₆로 암호화된 콘텐츠 키 데이터 Kc, UCP 데이터(106), 및 EMD 서비스 센터(102)의 서명 데이터를 저장하는 키 파일 KF를 생성하고, 키 파일 KF를 콘텐츠 제공기(101)에 보낸다.

서명 데이터는 키 파일 KF의 완전성 및 키 파일 KF의 생성자의 아이덴티티, 및 EMD 서비스 센터(102) 내의 키 파일 KF의 공식 등록을 검증하기 위해 사용된다.

콘텐츠 제공기(101)는 콘텐츠 키 데이터 Kc를 사용하여 콘텐츠 데이터 C를 암호화함으로써 콘텐츠 파일 CF를 생성하고, 콘텐츠 파일 CF, EMD 서비스 센터(102)로부터 수신된 키 파일 KF, 및 콘텐츠 제공기(102)의 서명 데이터를 저장하는, 안전한 컨테이너(104)(본 발명의 모듈에 대응함)를 인터넷, 또는 디지털 방송과 같은 네트워크, 또는 기록 매체와 같은 패키지 매체를 통해 사용자 홈 네트워크(103)에 분배한다.

안전한 컨테이너(104)에 저장된 서명 데이터는 대응하는 데이터의 완전성 및 데이터의 생성자 및 송신자의 아이덴티티를 검증하기 위해 사용된다.

사용자 홈 네트워크(103)는 예를 들어, 네트워크 장치(160₁), 및 오디오 - 비주얼(AV) 기기(160₂ 내지 160₄)를 포함한다. 네트워크 장치(160₁)는 내장된 SAM(105₁)을 갖는다. A/V 기기(160₂ 내지 160₄)는 각각 내장된 SAM(105₂ 내지 105₄)을 갖는다. SAM(105₁ 내지 105₄)은 IEEE - 1394 직렬 인터페이스 버스과 같은 버스(91)를 통해 서로 상호접속된다.

SAM(105₁ 내지 105₄)은 예를 들어, 네트워크를 통해 온라인으로 콘텐츠 제공기(101)로부터 수신된 안전한 컨테이너(101), 및/또는 대응하는 주기의 라이선스 키 데이터 KD₁ 내지 KD₆를 사용하여, 기록 매체를 통해 오프라인으로 콘텐츠 제공기(101)로부터 A/V 기기(160₂ 내지 160₄)로 공급된 안전한 컨테이너(104)를 디코딩한다.

SAM(105₁ 내지 105₄)에 공급된 안전한 컨테이너(104)는 안전한 컨테이너(104)의 구입/사용 모드가 사용자의 동작에 의해 결정된 후에 재생되거나또는 네트워크 장치(160₁) 및 A/V 기기(160₂ 내지 160₄) 내의 기록 매체 상에 기록될 준비가 된다.

SAM(105₁ 내지 105₄)는 사용 로그 데이터(108)로서 안전한 컨테이너(104)의 구입/사용 이력을 기록하고, 또한 구입 모드를 표시하는 사용 제어 상태(UCS) 데이터(166)를 생성한다.

사용 로그 데이터(108)는 예를 들어, EMD 서비스 센터(102)로부터의 요구에 응답하여, 사용자 홈 네트워크(103)로부터 EMD 서비스 센터(102)에 보내진다. UCS 데이터(166)는 예를 들어 구입 모드가 결정될 때마다, 사용자 홈 네트워크(103)로부터 EMD 서비스 센터(102)에 보내진다.

EMD 서비스 센터(102)는 사용 로그 데이터(108)에 기초한 계산 콘텐츠즈를 결정(계산)하고, 지불 게이트웨이(90)를 통해, 은행과 같은 결제 기구(91)를 사용하여, 계산된 계산 콘텐츠즈에 기초하여, 계산을 결제한다. 이 결제에 따라, 사용자 홈 네트워크(103)의 사용자에게 의해 결제 기구(91)에 이루어진 지불은 EMD 서비스 센터(102)에 의해 수행된 결제 처리에 의해 콘텐츠 제공기(101)에 주어진다. EMD 서비스 센터(102)는 결제 보고 데이터(107)를 콘텐츠 제공기(101)에 정기적으로 보낸다.

본 실시예에서, EMD 서비스 센터(102)는 인증 기능, 키 - 데이터 관리 기능, 및 권리 처리(이익 분배) 기능을 갖는다.

특히, EMD 서비스 센터(102)는 중립 최고 당국인 루트 증명 당국(92) 보다 낮은 층에 배치된 제2 증명 당국의 역할을 하고, EMD 서비스 센터(102)의 개인 키 데이터를 사용하여 공개 키 데이터의 공개 - 키 증명 데이터에 서명을 부착함으로써 공개 키 데이터를 인증한다. 공개 키 데이터는 콘텐츠 제공기(101) 및 SAM(105₁, 내지 105₄)내의 서명 데이터의 완전성을 검증하기 위해 사용된다. 상술한 바와 같이, EMD 서비스 센터(102)는 EMD 서비스 센터(102)의 인증 기능의 일부인 콘텐츠 제공기(101)의 UCP 데이터(106)를 등록하고 인증한다.

EMD 서비스 센터(102)는 또한 라이선스 키 데이터 KD₁, 내지 KD₆와 같은 키 데이터를 관리하는 키 - 데이터 관리 기능을 갖는다.

EMD 서비스 센터(102)는 또한 다음의 권리 처리(이익 분배) 기능을 갖는다. EMD 서비스 센터(102)는 인증된 UCP 데이터(106) 및 SAM(105₁, 내지 105₄)로부터 입력된 사용 로그 데이터(108)에서 기술된 제안된 소매 가격(SRP)에 기초하여 사용자에게 의해 이루어진 콘텐츠의 구입 및 사용에 대한 계산을 결재하고, 사용자에게 의해 이루어진 지불을 콘텐츠 제공기(101)에 분배한다.

도 2는 안전한 컨테이너(104)의 개념을 개략적으로 도시한 도면이다.

안전한 컨테이너(104)는 도 2에 도시한 바와 같이, 콘텐츠 제공기(101)에 의해 생성된 콘텐츠 파일 CF 및 EMD 서비스 센터(102)에 의해 생성된 키 파일 KF를 저장한다.

콘텐츠 파일 CF에서, 헤더 및 콘텐츠 ID를 포함하는 헤더 데이터, 콘텐츠 키 데이터 Kc로 암호화된 콘텐츠 데이터 C, 및 콘텐츠 제공기(101)의 개인 키 데이터 K_{CP,S} 로 암호화된 서명 데이터가 저장된다.

키 파일 KF에서, 헤더 및 콘텐츠 ID를 포함하는 헤더 데이터, 라이선스 키 데이터 KD₁, 내지 KD₆로 암호화된 콘텐츠 키 데이터 Kc 및 UCP 데이터(106), 및 EMD 서비스 센터(102)의 개인 키 데이터 K_{ESC,S} 로 암호화된 서명 데이터가 저장된다.

도 2에서, UCP 데이터(106)는 라이선스 키 데이터 KD₁, 내지 KD₆로 암호화될 수 없고, 이 경우에, 콘텐츠 제공기(101)의 개인 키 데이터 K_{CP,S} 로 암호화된 서명이 UCP 데이터(106)에 부가된다.

EMD 시스템의 개별 소자의 상세가 아래에 설명된다.

[콘텐츠 제공기(101)]

EMD 서비스 센터(102)와 통신을 시작하기 전에, 콘텐츠 제공기(101)는 콘텐츠 제공기(101)에 의해 생성된 공개 키 데이터 K_{CP,P}, 및 EMD 서비스 센터(102) 내의 콘텐츠 제공기(101)의 (계산을 결재하기 위한) 은행 계좌 번호를 오프라인으로 등록하고, 독특한 식별자(ID 번호) CP_ID를 얻는다. 콘텐츠 제공기(101)는 또한 EMD 서비스 센터(102)로부터 EMD 서비스 센터(102)의 공개 키 데이터 K_{ESC,P} 및 루트 증명 당국(92)의 공개 키 데이터 K_{R-CA,P}를 수신한다.

콘텐츠 제공기(101)는 도 3a에 도시된 콘텐츠 파일 CF 및 콘텐츠 파일 CF의 서명 데이터 SIG_{6,CP}, 키 파일 데이터 베이스(118b)로부터 판독된 콘텐츠 파일 CF에 대응하는 키 파일 KF 및 도 3b에 도시된 키 파일 KF의 키 파일 KF의 서명 데이터, 저장 유닛(119)으로부터 판독된 콘텐츠 제공기(101)의 공개 - 키 증명 데이터 CER_{CP} 및 도 3c에 도시된 공개 - 키 증명 데이터의 서명 데이터 SIG_{1,ESC}를 저장하는 안전한 컨테이너(104)를 생성한다.

콘텐츠 제공기(101)는 도 1에 도시된 사용자 홈 네트워크(103)의 네트워크 장치(160₁)에 안전한 컨테이너(104)를 온라인 또는 오프라인으로 공급한다.

이 방식으로, 본 실시예에 따르면, 안전한 컨테이너(104)에 저장된 콘텐츠 제공기(101)의 공개 키 데이터 K_{CP,P}의 공개 키 증명서 CER_{CP}가 사용자 홈 네트워크(103)에 직접 보내진 인 - 밴드 시스템이 사용된다. 이것은 사용자가 공개 키 증명서 CER_{CP}를 획득하기 위해 EMD 서비스 센터(102)와 통신할 필요성을 없애 준다.

다르게는, 본 발명에서, 사용자 홈 네트워크(103)가 안전한 컨테이너(104) 내에 그것을 저장하는 것 대신에 EMD 서비스 센터(102)로부터 공개 키 증명 CER_{CP} 를 획득할 수 있는 아웃-오브-밴드 시스템이 사용될 수 있다.

본 실시예에서, 서명 데이터는 개인 키 $K_{CP,S}$, $K_{ESC,S}$, $K_{SAM,1}$ 내지 $K_{SM,4}$ 를 각각 사용하여 콘텐츠 제공기(101), EMD 서비스 센터(102), 및 SAM(105₁ 내지 105₄) 내의 서명용으로 사용되는 데이터를 해싱함으로써 발생된다. 해시 값들은 해시 기능을 사용하여 발생된다. 해시 기능에 따라, 서명용으로 사용된 데이터가 입력되고, 다음에 해시값들로 출력되는 선정된 비트 길이를 갖는 데이터로 압축된다. 해시값들(출력값들)로부터 입력값을 예측하기가 어렵고, 입력 데이터의 1 비트가 변화할 때, 해시값들의 많은 비트가 변화한다. 동일한 해시값을 갖는 입력 데이터를 찾기가 또한 어렵다.

안전 컨테이너(104) 내의 개별 데이터의 상세는 다음과 같다.

서명 데이터 SIG6,CP6,CP

서명 데이터 SIG_{6,CP} 는 콘텐츠 파일 CF의 생성자와 센터의 보전성(integrity)을 검증하기 위해 안전 컨테이너(104)의 목적지에서 사용된다.

서명 데이터 SIG7,CP7,CP

서명 데이터 SIG_{7,CP} 는 키 파일 KF의 센터의 보전성을 검증하기 위해 안전 컨테이너(104)의 목적지에서 사용된다. 키 파일 KF의 생성자의 보전성은 키 파일 KF 내의 서명 데이터 SIG_{K1,ESC} 에 기초하여 안전 컨테이너(104)의 목적지에서 검증된다. 서명 데이터 SIG_{K1,ESC} 는 또한 EMD 서비스 센터(102) 내의 키 파일 KF의 레지스트레이션(registration)을 검증하기 위해 사용된다.

콘텐츠 파일 CF

도 4는 도 3a에 도시된 콘텐츠 파일 CF의 상세를 나타낸 것이다.

콘텐츠 파일 CF는, 도 3a와 도 4에 도시된 바와 같이, 헤더 데이터, 암호화 유닛(114)으로부터 입력된 콘텐츠 키 데이터 Kc로 암호화된 메타 데이터 Meta, 콘텐츠 데이터 C, A/V 압축해제 소프트웨어 Soft, 및 디지털 워터마크 정보 모듈(Watermark Module) WM을 저장한다.

도 3a는 디지털 신호 프로세서(DSP)가 콘텐츠 데이터 C를 압축해제하기 위한 A/V 압축/압축해제 장치로서 사용될 때의 콘텐츠 파일 CF의 구성을 나타낸 것이다. DSP는 안전 컨테이너(104) 내의 A/V 압축해제 소프트웨어 및 디지털 워터마크 정보 모듈을 사용하여 안전 컨테이너(104) 내의 콘텐츠 데이터 C를 압축해제하고, 디지털 워터마크 정보를 삽입하여 검출한다. 이것은 컨테이너 제공자(101)가 디지털 워터마크 정보에 대해 원하는 압축 방법 및 삽입 방법을 사용할 수 있게 한다.

하드웨어 또는 사전 기억된 소프트웨어가 콘텐츠 데이터 C를 압축해제하고 디지털 워터마크 정보를 삽입 및 검출하기 위한 A/V 압축/압축해제 장치로서 사용되면, A/V 압축해제 소프트웨어 및 디지털 워터마크 정보 모듈은 콘텐츠 파일 CF 내에 저장되지 않을 수도 있다.

헤더 데이터는, 도 4에 도시된 바와 같이, 동기화 신호, 콘텐츠 ID, 콘텐츠 ID를 검증하기 위해 콘텐츠 제공자(101)의 전용 키 데이터 $K_{CP,S}$ 에 의해 얻어진 서명 데이터, 디렉토리 정보, 하이퍼링크 정보, 시리얼 번호에 관한 정보, 콘텐츠 파일 CF의 유효 기간 및 생성자, 파일 사이즈, 암호화 플래그, 암호화 알고리즘, 및 서명 알고리즘, 및 디렉토리 정보를 검증하기 위해 콘텐츠 제공자(101)의 전용 키 데이터 $K_{CP,S}$ 에 의해 얻어진 서명 데이터를 포함한다.

메타 데이터 Meta는, 도 4에 도시된 바와 같이, 프로덕트(즉, 콘텐츠 데이터 C)의 기술, 프로덕트 데몬스트레이션용 광고 정보, 프로덕트 관련 정보, 및 상기 정보를 검증하기 위한 콘텐츠 제공자의 서명 데이터를 포함한다.

본 발명에서, 메타 데이터 Meta는 도 3a 및 도 4에 도시된 바와 같이 콘텐츠 파일 CF 내에 저장되면서 송신된다. 대안적으로, 콘텐츠 파일 CF 내에 메타 데이터 Meta를 저장하는 대신에, 메타 데이터 Meta는 콘텐츠 제공자(101)로부터, 예를 들어 콘텐츠 파일 CF를 송신하는 경로와 다른 경로를 통해 SAM(105₁)으로 전송될 수 있다.

콘텐츠 데이터 C는 다음과 같은 방식으로 얻어진다. 소스 디지털 워터마크 정보(Source Watermark) W_S, 카피 제어 디지털 워터마크 정보(Copy Control Watermark) W_C, 사용자 디지털 워터마크 정보(User Watermark) W_L, 및 링크 디지털 워터마크 정보(Link Watermark) 등은 예를 들어 콘텐츠 마스터 소스 데이터베이스로부터 판독된 콘텐츠 데이터 내에 삽입된다. 그 다음, 콘텐츠 데이터는 ATRAC3(Adaptive Transform Acoustic Coding 3)(상표명)과 같은 음성 압축 방법에 따라 압축되고, 공통 키로서 콘텐츠 키 Kc를 사용함으로써 DES(Data Encryption Standard) 또는 Triple DES와 같은 공통 키 암호 시스템에 따라 암호화된다.

콘텐츠 키 데이터 Kc는 예를 들어, 난수(random number) 발생기를 사용함으로써 선정된 비트 수를 갖는 난수를 발생시켜 얻어진다. 콘텐츠 키 데이터 Kc는 콘텐츠 데이터에 의해 제공된 음악에 관한 정보로부터 발생될 수 있다. 콘텐츠 키 데이터 Kc는 정기적으로 갱신된다.

다수의 콘텐츠 제공자(101)가 존재할 때, 각각의 콘텐츠 제공자(101)에게 유일한 콘텐츠 키 데이터 Kc가 사용될 수 있고, 또는 공통 콘텐츠 키 데이터 Kc가 모든 콘텐츠 제공자(101)에게 사용될 수 있다.

소스 디지털 워터마크 정보 W_S는 콘텐츠 데이터의 저작권 소유자의 이름과 같은 저작권에 관한 정보, ISRC(International Standard Recording Code), 오서팅(authoring) 데이터, 오서팅 머신 식별 데이터(ID), 및 콘텐츠의 분산 목적지를 나타낸다.

카피 제어 디지털 워터마크 정보 W_C는 아날로그 인터페이스를 통한 카펅 동작을 금지하기 위한 카피 금지 비트를 포함하는 정보를 나타낸다.

사용자 디지털 워터마크 정보 W_L는, 예를 들어 안전 컨테이너(104)의 분산 소스 및 분산 목적지를 지칭하는 콘텐츠 제공자(101)의 식별자 CP_ID, 및 각각 사용자 홈 네트워크(103)의 SAM(105₁, 내지 105₄)의 식별자 SAM_ID₁ 내지 SAM_ID₄를 포함한다.

링크 디지털 워터마크 정보 W_L은, 예를 들어 콘텐츠 데이터 C의 콘텐츠 ID를 포함한다. 링크 디지털 워터마크 정보 W_L을 콘텐츠 데이터 C 내에 삽입함으로써, 텔레비전 방송 또는 진폭 변조(AM)/주파수 변조(FM) 라디오 방송과 같은 아날로그 방송을 통해 분산된 콘텐츠 데이터의 경우에도, 사용자로부터의 요청에 응답하여, EMD 서비스 센터(102)는 콘텐츠 데이터 C를 다루는 콘텐츠 제공자(101)를 사용자에게 안내할 수 있다. 즉, 콘텐츠 데이터 C의 수신측은 디지털 워터마크 정보 디코더를 사용함으로써 콘텐츠 데이터 C 내에 삽입된 링크 디지털 워터마크 정보 W_L을 검출하고, 검출된 콘텐츠 ID를 EMD 서비스 센터(102)에 송신한다. 이것은 EMD 서비스 센터(102)가 콘텐츠 데이터 C를 다루는 콘텐츠 제공자(101)를 사용자에게 안내할 수 있게 한다.

더욱 구체적으로, 지금 사용자가 자동차 안에서 방송 중인 음악을 듣고, 이것에 흥미를 느껴서, 선정된 버튼을 누른다고 하자. 그러면, 라디오 내에 내장된 디지털 워터마크 정보 디코더가 콘텐츠 데이터 C 내에 삽입된 링크 디지털 워터마크 정보 W_L 내에 포함된 콘텐츠 ID, 및 콘텐츠 데이터 C를 레지스터하는 EMD 서비스 센터(102)의 통신 어드레스를 검출한다. 그 다음, 디지털 워터마크 정보 디코더는 휴대용 매체, 예를 들면 미니 디스크(MD)(상표명)와 같은 광 디스크 또는 메모리 스틱(상표명)과 같은 반도체 메모리 내에 로드된 매체 SAM 상에 검출된 데이터를 기록한다. 그 다음, 휴대용 매체는 네트워크에 접속된 SAM이 로드된 네트워크 장치 내에 설정된다. SAM과 EMD 서비스 센터(102) 사이의 상호 인증을 실행한 후에, 매체 SAM 내에 저장된 ID 정보 및 기록된 콘텐츠 ID는 네트워크 디바이스로부터 EMD 서비스 센터(102)로 보내진다. 그 다음, 네트워크 디바이스는 콘텐츠 제공자(101)와 같이 콘텐츠 데이터 C를 다루는 콘텐츠 제공자의 리스트를 EMD 서비스 센터(102)로부터 수신한다.

대안적으로, 사용자로부터의 콘텐츠 ID에 응답하여, EMD 서비스 센터(102)는 콘텐츠 ID에 대응하는 콘텐츠 데이터 C를 다루는 콘텐츠 제공자(101)에게 사용자의 정보를 보낼 수 있다. 상술된 정보를 수신할 때, 사용자가 이미 콘텐츠

제공자(101)와 접촉했다는 것이 발견되면, 콘텐츠 제공자(101)는 콘텐츠 데이터 C를 사용자의 네트워크 디바이스에 보낼 수 있다. 그렇지 않으면, 콘텐츠 제공자(101)는 콘텐츠 제공자(101)의 프로모션 정보를 사용자의 네트워크 디바이스에 보낼 수 있다.

본 발명의 제2 실시예(후술됨)에서는, 링크 디지털 워터마크 정보 W_1 에 기초하여, EMD 서비스 센터(102)는 콘텐츠 데이터 C를 다루는 서비스 제공자(310)를 사용자에게 안내할 수 있다.

양호하게, 제1 실시예에서, 디지털 워터마크 정보의 콘텐츠 및 삽입 위치는 EMD 서비스 센터(102) 내에 래지스터되어 관리될 수 있는 디지털 워터마크 정보 모듈 WM으로서 정해질 수 있다. 디지털 워터마크 정보 모듈 WM은, 예를 들어 사용자 홈 네트워크(103) 내의 네트워크 디바이스(160_1) 및 A/V 머신(160_2 내지 160_4)에 의해 디지털 워터마크 정보를 검증하기 위해 사용된다.

더욱 구체적으로, 사용자 홈 네트워크(103)는 EMD 서비스 센터(102)에 의해 관리된 사용자 디지털 워터마크 정보 모듈 WM에 기초하여, 사용자 홈 네트워크(103)에 의해 검증된 디지털 워터마크 정보의 콘텐츠 및 삽입 위치가 EMD 서비스 센터(102)에 의해 관리된 것과 일치하는지의 여부를 판정한다. 검증된 정보가 EMD 서비스 센터(102)의 것과 일치하면, 디지털 워터마크 정보는 정당한 것이라고 판정된다. 그러므로, 정당하게 삽입된 디지털 워터마크 정보를 높은 확률로 검증할 수 있다.

ATRAC3 압축해제 소프트웨어일 수 있는 A/V 압축해제 소프트웨어 Soft는 사용자 홈 네트워크(103)의 네트워크 디바이스(160_1) 및 A/V 머신(160_2 내지 160_4) 내의 콘텐츠 파일 CF를 압축해제하는 데 사용된다.

이것은 안전 컨테이너(104) 내에 저장된 A/V 압축해제 소프트웨어를 사용함으로써 단순히 SAM(105_1 내지 105_4)이 콘텐츠 데이터 C를 압축해제할 수 있게 한다. 따라서, 상이한 압축/압축해제 방법이 콘텐츠 데이터 C의 개별 아이템에 대해, 또는 개별 콘텐츠 제공자에 대해 설정되는 경우라도, 콘텐츠 데이터 C를 압축해제하는 과도한 부담이 사용자에게 가해지지 않는다.

콘텐츠 파일 CF는, 도 4에 도시된 바와 같이, 파일 판독기, 및 전용 키 $K_{CF,S}$ 를 사용하여 파일 판독기를 검증하기 위한 서명 데이터를 포함할 수 있다. 이것은 SAM(105_1 내지 105_4)이 콘텐츠 파일 CF의 상이한 포맷을 저장하는 다수의 상이한 유형의 안전 컨테이너(104)를 효율적으로 처리할 수 있게 한다.

파일 판독기는 콘텐츠 파일 CF 및 대응하는 키 파일 KF를 판독하는 데 사용되고, 이들 파일의 판독 절차를 지시한다.

이 실시예에서는, 파일 판독기가 EMD 서비스 센터(102)에서 SAM(105_1 내지 105_4)으로 보내지는 것으로 하였으므로, 안전 컨테이너(104)의 콘텐츠 파일 CF는 파일 판독기를 저장하지 않는다.

이 실시예에서, 암호화된 콘텐츠 데이터 C는 압축 플러그, 즉 콘텐츠 C가 압축되었는지의 여부, 콘텐츠 데이터 C의 압축 방법, 암호화 방법(공통 키 암호시스템 및 공개 키 암호시스템을 포함함), 콘텐츠 데이터 C의 신호 소스(예를 들어, 샘플링 주파수), 및 서명-데이터 생성 방법(알고리즘)과 같은 팩트에 상관없이 안전 컨테이너(104) 내에 저장된다. 즉, 상술된 팩트는 콘텐츠 제공자(101)의 자유 제량으로 결정될 수 있다.

키 파일 KF

도 5는 도 3b에 도시된 키 파일 KF의 상세를 나타낸 것이다.

이 실시예에서, 예를 들어, 레지스트레이션 프로세싱이 레지스트레이션 모듈 Mod_2 을 콘텐츠 제공자(101)에서 EMD 서비스 센터(102)로 전송함으로써 실행된 후에, 도 6에 도시된 바와 같이, 6개월의 키 파일 KF는 예를 들어, EMD 서비스 센터(102)에서 콘텐츠 제공자(101)로 보내져서, 키 파일 데이터베이스 내에 저장된다. 레지스트레이션 모듈 Mod_2 및 키 파일 KF의 송신 및 수신 시에, 상호 인증은 콘텐츠 제공자(101)와 EMD 서비스 센터(102) 사이에서 실행되고, 레지스트레이션 모듈 Mod_2 및 키 파일 KF는 세션 키 데이터 K_{SES} 를 사용하여 암호화되고 해독된다.

키 파일 KF는 각각의 콘텐츠 데이터 C에 제공되어, 후술되는 콘텐츠 파일 CF의 헤더 내의 디렉토리 구조 데이터 DSD에 따라 대응하는 콘텐츠 파일 CF에 링크된다.

키 파일 KF는, 도 3b 및 도 5에 도시된 바와 같이, 헤더, 콘텐츠 키 데이터 K_c , UCP 데이터(라이선스 등의 조건)(106), SAM 프로그램 다운로드 컨테이너(SDC_1 내지 SDC_3), 및 서명 데이터 $SIG_{K1,ESC}$ 를 저장한다.

EMD 서비스 센터(102)의 전용 키 $K_{ESC,S}$ 를 사용하여 얻어진 서명 데이터는 도 3b에 도시된 바와 같이 키 파일 KF 내에 저장된 모든 데이터에 대한 서명 데이터 $SIG_{K1,ESC}$ 일 수 있다. 대안적으로, 서명 데이터는 도 5에 도시된 바와 같이 헤더에서 키 파일로의 정보에 대해, 콘텐츠 키 K_c 및 UCP 데이터(106)에 대해, 및 SAM 프로그램 다운로드 컨테이너 SDC 에 대해 따로따로 제공될 수 있다.

콘텐츠 키 데이터 K_c 및 UCP 데이터(106), 및 SAM 프로그램 다운로드 컨테이너 SDC_1 내지 SDC_3 은 대응하는 기간의 라이선스 키 데이터 KD_1 내지 KD_3 을 사용하여 암호화된다.

UCP 데이터(106)는 라이선스 키 데이터에 의해 암호화되지 않은 서명 데이터가 구비된 경우에, 키 파일 KF 내에 저장되지 않을 수 있다.

헤더 데이터는 도 5에 도시된 바와 같이 동기화 신호, 콘텐츠 ID, EMD 서비스 센터(102)의 전용 키 $K_{ESC,S}$ 를 사용하여 콘텐츠 ID를 검증하기 위한 서명 데이터, 디렉토리 구조 데이터, 하이퍼링크 데이터, 키 파일 KF에 관한 정보, 및 EMD 서비스 센터(102)의 전용 키 $K_{ESC,S}$ 를 사용하여 디렉토리 구조 데이터를 검증하기 위한 서명 데이터를 포함한다.

여러가지 유형의 정보가 헤더 데이터 내에 포함될 수 있으며, 상황에 따라 변할 수 있다. 예를 들어, 도 7에 도시된 정보가 포함될 수 있다.

콘텐츠 ID는 도 8에 도시된 정보를 저장할 수 있다. 콘텐츠 ID는 EMD 서비스 센터(102) 또는 콘텐츠 제공자(101)내에 생성되고, 도 8에 도시된 것과 같은, EMD 서비스 센터의 비공개 키 데이터 $K_{ESC,S}$ 를 사용하여 얻어진 서명 데이터(signature data) 또는 콘텐츠 제공자(101)의 비공개 키 데이터 $K_{CP,S}$ 를 사용하여 얻어진 서명 데이터가 콘텐츠 ID에 부착된다. 콘텐츠 ID는 콘텐츠 제공자(101) 또는 EMD 서비스 센터(102)중의 하나에서 생성될 수 있다.

디렉토리 구조 데이터는 보안 컨테이너(104)내의 키 파일 KF와 콘텐츠 파일 CF사이 및 콘텐츠 파일들 CF 사이의 관계를 나타낸다.

예를 들면, 콘텐츠 파일 CF_1 내지 CF_3 및 대응하는 키 파일 KF_1 내지 KF_3 가 보안 컨테이너(104)내에 저장된다면, CF_1 내지 CF_3 사이의 링크 및 콘텐츠 파일 CF_1 내지 CF_3 와 키 파일 KF_1 내지 KF_3 사이의 링크가 도 9에 도시된 바와 같이 디렉토리 구조 데이터에 의해 설정된다.

하이퍼링크 데이터는 보안 컨테이너(104) 내의 모든 파일을 고려함으로써 키 파일 KF의 계층적 구조 및 콘텐츠 파일 CF와 키 파일 KF사이의 관계를 나타낸다.

좀 더 구체적으로, 도 10에 도시된 것과 같이, 각각의 콘텐츠 파일 CF 및 각각의 키 파일 KF에 대해 링크될 어드레스 정보 및 그의 인증값(해시값(hash value))이 보안 컨테이너(104)내에 저장된다. 그 후, 해시 함수 $H(x)$ 에 의해 얻어진 하나의 콘텐츠 파일 CF 또는 하나의 키 파일 KF의 해시값이 링크될 다른 콘텐츠 파일 CF 또는 다른 키 파일 KF의 해시값과 비교됨으로써, 파일들사이의 링크를 검증한다.

UCP 데이터(106)는 콘텐츠 데이터 C, 예를 들면, 콘텐츠 제공자(101)의 조작자가 희망하는 복사 규칙 및 제한된 소 매상의 가격(SRP)의 동작 규칙을 정의하는 기술자(descriptor)이다.

좀 더 구체적으로, UCP 데이터(106)는, 도 5에 도시된 것과 같이, 콘텐츠 ID, 콘텐츠 제공자(101)의 식별기 CP_ID, UCP 데이터(106)의 효과값, EMD 서비스 센터(102)의 통신 어드레스, 유스-스페이스 연구 정보(use-space research information), SRP, 사용 방법, UCS 정보, 제품을 선전하기 위한 UCS 정보, 및 상술한 정보에 대한 서명 데이터를 포함한다.

UCS 정보는 다양한 구매 모드, 예를 들면, 재분배, 사용한 만큼 지불, 판매(sell through), 시간 제한적인 판매, 플레이 N당 판매 지불, 시간당 지불, SCMS 디바이스에 대한 사용당 지불, 블록당 지불 등으로부터 선택된 수용된 구매 모드를 나타낸다.

서비스 제공자(310)를 통해 사용자 홈 망(303)으로 보안 컨테이너(304)를 전송하는, 다음에 설명되는, 제2 실시예에서, UCP 데이터(106)는 콘텐츠 제공자(301)에 의해 보안 컨테이너(104)가 제공되는 서비스 제공자(310) SP_ID의 식별기를 포함한다.

SAM 프로그램 다운로드 컨테이너 SDC₁ 내지 SDC₃은, 도 5에 도시된 바와 같이, SAMs 105₁ 내지 105₃, UCP-L(라벨)과 같은 라벨 판독기내에 프로그램을 다운로드하기 위한 절차를 나타내는 다운로드 드라이버를 저장한다. UCP 데이터(U106)의 구분(문법)을 나타내는 R(판독기), 저장 유닛(192) 마스크 롬(1104) 또는 비휘발성 메모리(105)와 같은 플래시 판독 전용 메모리(롬))내에 저장된 각각의 블록 데이터의 삭제 및 기록의 잠금 또는 해제하기 위한 잠금 키 데이터는 SAMs 105₁ 내지 105₃ 및 상술한 정보에 대한 서명 데이터내에 내장된다. 마스크 롬(1104) 또는 비휘발성 메모리(1105)는 잠금 키 데이터에 기초하여 블록 유닛내의 저장 데이터의 삭제 및 기록을 제어한다.

콘텐츠 제공자(101)로부터 사용자 홈 망(103)으로 보안 컨테이너(104)가 공급되는 모드에 대해 설명된다.

상술한 바와 같이, 콘텐츠 제공자(101)는 사용자 홈 망(103)에 온라인 또는 오프라인으로 보안 컨테이너(104)를 공급한다.

콘텐츠 제공자(101)가 사용자 홈 망(103)의 망 디바이스(160₁)로 온라인을 통해 보안 컨테이너(104)를 제공할 경우, 다음의 과정이 취해진다. 콘텐츠 제공자(101)는 세션 키(공통 키) K_{SES}를 공유하고 세션 키 K_{SES}를 사용하여 보안 컨테이너(104)를 암호화하여 EMD 서비스 센터(102)로 전송하도록 망 디바이스(160₁)로 상호 인증한다. 세션 키 K_{SES}는 상호 인증이 실행될 때마다 새롭게 생성된다.

보안 컨테이너(104)를 전송하기 위한 통신 프로토콜로서, 멀티미디어 및 하이퍼미디어 정보 코딩 전문가 그룹(MHEG) 프로토콜이 디지털 방송용으로 사용되거나 확장 가능한 마크업 언어(XML), 동기된 멀티 미디어 통합 언어(SMIL), 또는 하이퍼텍스트 마크업 언어(HTML)가 인터넷용으로 사용될 수 있다. 보안 컨테이너(104)는 코딩 방법에 의존하지 않고 터널링 기술에 따라 대응하는 프로토콜내에 내장된다.

따라서, 보안 컨테이너(104)의 포맷은 통신 프로토콜과 일치할 필요가 없기 때문에 보안 컨테이너(104)의 포맷의 선택시 유연성이 증가된다.

콘텐츠 제공자(101)로부터 사용자 홈 망(103)으로 보안 컨테이너(104)를 전송하기 위해 사용되는 통신 프로토콜은 상술한 프로토콜에 한정되지 않는다.

본 실시예에서, 모듈이 콘텐츠 제공자(101), EMD 서비스 센터(102), 및 상호 통신하기 위한 망 디바이스(160₁)내에 포함됨에 따라, 모니터링되는 것을 방지하는 조치가 없고 조치가 방지되는 통신 게이트웨이 사용된다.

대조적으로, 콘텐츠 제공자(101)가 보안 컨테이너(104)를 사용자 홈 망(103)에 오프라인으로 공급할 경우, 보안 컨테이너(104)는 다음에 상세히 설명될 기록 매체(롬 또는 램)상에 기록되고, 그 후, 램 또는 롬내의 콘텐츠는 통신 경로를 통해 사용자 홈 망(103)으로 공급된다.

도 11은 본 실시예에서 사용된 기록 매체(롬)(130₁)을 도시한다.

기록 매체(롬)(130₁)는 롬 영역(131), 보안 램 영역(132), 및 매체 SAM(133)을 구비한다. 도 3a에 도시된 콘텐츠 파일 CF는 롬 영역(131)내에 저장된다.

보안 램 영역(132)은 액세스하기 위해 소정의 허가(인증)을 필요로 하는 영역이고, 도 3b에 도시된 키 파일 KF, 도 3c에 도시된 공개-키 증명 데이터 CER_{CP}, 및 기계의 유형에 따라 고유값을 갖는 저장 키 데이터 K_{STR}를 변수로 사용하고, 메시지 인증 코드(MAC) 함수를 사용함으로써 생성된 서명 데이터를 저장한다. 또한, 보안 램 영역(132)은 기록 매체에 대해 고유값을 갖는 매체 키 데이터 K_{MED}를 사용함으로써 키 파일 KF 및 공개-키 증명 데이터 CER_{CP}를 암호화하여 얻어지는 데이터를 저장한다.

또한, 보안 램 영역(132)은 불법 동작에 의해 무효가 되는 SAMs 105₁ 내지 105₃ 및 콘텐츠 제공자(101)를 기술하기 위한 공개 키 증명 취소 데이터를 저장한다.

다음에 설명되는, 본 실시예에서 사용되는 매체 SAM과 매체 드라이브 SAM(260)사이의 통신에서, 하나의 SAM은 그 취소 리스트를 다른 SAM의 취소 리스트와 비교하고 리스트들이 생성될 때를 결정한다. 미리 생성된 취소 리스트는 다른 취소 리스트에 의해 갱신된다.

보안 램 영역(132)은 콘텐츠 데이터 C의 구매/사용 모드가 사용자 홈 망(103)의 SAMs 105₁ 내지 105₃ 내에서 결정될 경우 생성되는 UCS 데이터(166)를 저장한다. 보안 램 영역(132)내에 UCS 데이터(166)를 저장함으로써 구매/사용 모드가 결정되는 기록 매체(롬)(130₁)이 제공될 수 있다.

매체 SAM(133)은, 예를 들면, 기록 매체(롬)(130₁)의 식별기인 미디어 ID, 및 매체 키 데이터 K_{MED}를 저장한다. 매체 SAM(133)은, 예를 들면, 상호 인증 기능을 가진다.

본 실시예에서 사용가능한 기록 매체(롬)은 또한 도 12에 도시된 기록 매체(롬)(130₂) 또는 도 13에 도시된 기록 매체(롬)(130₃)일 수 있다.

도 12에 도시된 기록 매체(롬)(130₂)은 인증 기능을 갖는 매체 SAM(133) 및 롬 영역(131)을 가지나, 도 11에 도시된 기록 매체(롬)(130₁)과 달리, 보안 램 영역(132)이 구비되지 않는다. 기록 매체(롬)(130₂)이 사용된다면, 콘텐츠 파일 CF는 롬 영역(131)내에 저장되고 키 파일 KF는 매체 SAM(133)내에 저장된다.

도 13에 도시된 기록 매체(롬)(130₃)은 롬 영역(131) 및 보안 램 영역(132)을 가지나, 도 11에 도시된 기록 매체(롬)(130₁)과 달리, 매체 SAM(133)은 구비되지 않는다. 기록 매체(롬)(130₃)이 사용된다면, 콘텐츠 파일 CF는 롬 영역(131)내에 저장되고 키 파일 KF는 매체 SAM(132)내에 저장된다. 인증은 대응하는 SAM으로 실행되지 않는다.

롬 기록 매체 대신에, 램 기록 매체가 본 실시예에 사용될 수 있다.

본 실시예에 사용 가능한 램 기록 매체로서, 도 14에 도시된 것과 같이, 매체 SAM(133)을 구비한 기록 매체(램)(130₄), 보안 램 영역(132), 및 비보안 램 영역(134)이 사용될 수 있다. 상기 기록 매체(램)(130₄)에서, 매체 SAM은 인증 기능을 가지고, 보안 램 영역(132)는 키 파일 KF를 저장한다. 비보안 램 영역(134)은 콘텐츠 파일 CF를 저장한다.

선택적으로, 도 15에 도시된 기록 매체(램)(130₅) 및 도 16에 도시된 기록 매체(램)(130₆)이 사용될 수 있다.

도 15에 도시된 기록 매체(램)(130₅)는 비보안 램 영역(134) 및 인증 기능을 갖는 매체 SAM(133)을 포함하나, 도 14에 도시된 기록 매체(램)(130₄)와 달리, 보안 램 영역(132)이 구비되지 않는다. 기록 매체(램)(130₅)를 사용할 경우, 콘텐츠 파일 CF는 비보안 램 영역(134)내에 저장되고, 키 파일 KF는 매체 SAM(133)내에 저장된다.

기록 매체(램)(130_g)는 보안 램 영역(132) 및 비보안 램 영역(134)을 포함하나, 도 14에 도시된 기록 매체(램)(130_g)와 달리, 매체 SAM(133)을 구비하지 않는다. 기록 매체(램)(130_g)을 사용할 경우, 콘텐츠 파일 CF는 비보안 램 영역(134)에 저장되고 키 파일 KF는 보안 램 영역(132)내에 저장된다. 인증은 대응하는 SAM으로 실행되지 않는다.

상술한 바와 같이, 콘텐츠 데이터 C가, 예를 들면, 기록 매체(130_j)를 사용하여 콘텐츠 제공자(101)로부터 사용자 홈 망(103)으로 망을 통한 온라인 또는 오프라인으로 분배될 지 여부에 상관없이 콘텐츠 데이터 C를 분배하기 위해 UCP 데이터(106)를 저장하는 보안 컨테이너(104)의 공통 포맷이 사용된다. 이는 사용자 홈 망(103)의 SAMs 105_j 내지 105_k로 하여금 공통 UCP 데이터(106)에 기초하여 정상 처리(rights processing)를 실행한다.

또한, 상술한 바와 같이, 본 실시예에서, 콘텐츠 키 데이터 Kc로 암호화된 콘텐츠 데이터 C가 보안 컨테이너(104)내에서 콘텐츠 데이터 C를 암호 해제하기 위한 콘텐츠 키 데이터 Kc와 함께 저장되는 대역내 시스템(in-band system)이 사용된다. 상기 대역내 시스템에 따르면, 사용자 홈 망(103)이 콘텐츠 데이터 C를 다시 플레이할 경우 콘텐츠 키 데이터 Kc를 분리하여 분배할 필요가 없기 때문에 망 통신의 부담을 감소시킨다. 콘텐츠 키 데이터 Kc는 라이선스 키 데이터 KD₁ 내지 KD₂로 암호화된다. 그러나, 라이선스 키 데이터 KD₁ 내지 KD₂는 EMD 서비스 센터(102)내에서 관리되고 SAMs 105_j 내지 105_k가 먼저 EMD 서비스 센터(102)를 액세스할 경우 사용자 홈 망(103)의 SAMs 105_j 내지 105_k로 이미 분배되어 있다. 이는 사용자 홈 망(103)으로 하여금 온라인으로 EMD 서비스 센터(102)를 액세스하지 않고 오프라인으로 콘텐츠 데이터 C를 사용하는 것을 가능케 한다.

본 발명에서는, 아래에서 설명될, 콘텐츠 데이터 C 및 콘텐츠 키 데이터 Kc가 사용자 홈 망(103)에 분리되어 공급되는 대역외 시스템(out-of-band system)이 사용될 수 있다.

콘텐츠 제공자(101)에 의해 보안 컨테이너(104)를 생성하기 위한 공정은 다음과 같다.

도 17 내지 19는 상술한 공정을 도시하기 위한 플로우 차트이다.

단계 S17-1(도 17)에서, 콘텐츠 제공자(101)는, 계정을 처리하기 위한 은행 계좌 또는 콘텐츠 제공자(101)의 ID 증명을 사용함으로써 EMD 서비스 센터(102)내에 오프라인으로 등록하고, 광범위한 고유 식별자 CP_ID를 획득한다. 콘텐츠 제공자(101)는 EMD 서비스 센터(102)로부터 콘텐츠 제공자(101)의 공개 키 증명 CER_{CP}을 이미 획득하였다.

단계 17-2에서, 콘텐츠 제공자(101)는 인증되고 레거시 콘텐츠 데이터(legacy content data)로 미리 저장된 콘텐츠 마스터 소스를 디지털화 하고 상기 데이터로 콘텐츠 ID를 할당한다. 그 후, 콘텐츠 마스터 소스는 콘텐츠 마스터 소스내에 저장되고 중점적으로 관리된다.

그 다음, 단계 17-3에서, 콘텐츠 제공자(101)는 중점적으로 관리되는 콘텐츠 마스터 소스의 각각에 대해 메타 데이터 META를 발생시키고 메타 데이터베이스내에 저장한다.

순차적으로, 단계 17-4에서, 콘텐츠 제공자(101)는 콘텐츠 데이터, 즉, 콘텐츠 마스터 소스를 콘텐츠 마스터 소스 데이터베이스로부터 판독하고 콘텐츠 데이터내에 디지털 워터마크 정보를 삽입한다.

단계 17-5에서, 콘텐츠 제공자(101)는 소정의 데이터베이스내에 단계 17-4에서 삽입된 디지털 워터마크의 내장된 위치 및 콘텐츠를 저장한다.

그러면, 단계 S17-6에서 내장 디지털 워터마크 정보를 구비한 콘텐츠 데이터가 압축된다. 단계 S17-7에서 콘텐츠 제공자(101)는 단계 S17-6에서 압축된 콘텐츠 데이터를 압축 해제하여 콘텐츠 데이터를 생성한다. 단계 S17-8에서 콘텐츠 제공자(101)는 압축된 콘텐츠 데이터에 대한 오디오 검사를 수행한다.

이후, 단계 S17-9에서 콘텐츠 제공자(101)는 단계 S17-5에서 데이터베이스에 저장된 디지털 워터마크 정보의 콘텐츠 및 내장 위치에 기초하여 콘텐츠 데이터에 내장된 디지털 워터마크를 검출한다. 오디오 검사와 디지털 워터마크 정보의 검출이 성공적으로 수행되었다면 콘텐츠 제공자(101)는 단계 S17-10(도 18)의 처리를 실행한다. 상기 설명한 프로세스의 하나라도 실패하였다면 단계 S17-4의 처리가 반복된다.

단계 S17 - 10 에서 콘텐츠 제공자 (101)는 콘텐츠 키 데이터 Kc 를 생성하기 위해 임의의 수를 발생시키고 이를 보호한다. 콘텐츠 제공자 (101)는 또한 콘텐츠 키 데이터 Kc를 활용하여 단계 S17 - 6 에서 압축된 콘텐츠 데이터를 암호화한다. 단계 S17 - 11에서 콘텐츠 제공자 (101) 는 도 3a 에 도시된 콘텐츠 파일 CF 를 생성하고 이를 콘텐츠 파일 데이터베이스에 저장한다.

그후 단계 17 - 12 에서 콘텐츠 제공자 (101)는 콘텐츠 데이터 C 에 관한 UCP 데이터 (106) 를 생성한다. 단계 S17 - 13 에서 콘텐츠 제공자 (101)는 SRP 를 결정하고 이를 데이터베이스 내에 저장한다. 단계 S17 - 14 에서 콘텐츠 제공자 (101)는 콘텐츠 ID, 콘텐츠 키 데이터 Kc, 및 UCP 데이터 (106)를 EMD 서비스 센터 (102)로 출력한다. 다음으로, 단계 S17 - 15에서 콘텐츠 제공자 (101)는 EMD 서비스 센터 (102)로부터 라이선스 키 데이터인 KD₁에서 KD₃에 의해 암호화된 키 파일 KF를 수신한다. 단계 S17 - 16 에서 콘텐츠 제공자 (101)는 키 파일 데이터베이스에 수신된 키 파일 KF를 저장한다. 단계 S17 - 17에서 (도 19) 콘텐츠 제공자 (101)은 콘텐츠 파일 CF 및 키 파일 KF를 하이퍼링크한다. 단계 S17 - 18 에서 콘텐츠 제공자 (101)는 개인 키 데이터 K_{CP,S}를 사용하여 콘텐츠 파일 CF의 해쉬 (hash) 값으로부터 서명 데이터 SIG_{6,CP}를 생성한다. 콘텐츠 제공자 (101)는 또한 개인 키 데이터 K_{CP,S}를 사용하여 키 파일 KF의 해쉬 값으로부터 서명 데이터 SIG_{7,CP}를 생성한다.

단계 S17 - 19 에서 콘텐츠 제공자 (101) 는 도 3 a 에서 도 3 c 에 도시된 대로 콘텐츠 파일 CF, 키 파일 KF, 공개 키 인증 데이터 CER_{CP}, 서명 데이터 SIG_{6,CP}, SIG_{7,CP}, 및 SIG_{1,ESC} 을 저장한 보안 컨테이너 (104)를 발생시킨다.

콘텐츠 데이터가 다수의 보안 컨테이너들을 포함하는 복합 포맷으로 제공되는 것이 요구된다면 각각의 보안 컨테이너 (104)는 단계 S17 - 1에서 S17 - 19 까지의 처리를 반복함으로써 생성된다. 그러면, 단계 S17 - 20 에서 콘텐츠 파일 CF 및 키 파일 KF 사이의 관계가 하이퍼링크되고 또한 콘텐츠 파일 CF 사이의 관계가 하이퍼링크된다. 그 후 단계 S17 - 21에서 콘텐츠 제공자 (101)는 생성된 보안 컨테이너 (104)를 보안 컨테이너 데이터베이스에 저장한다.

[EMD 서비스 센터 102]

도 20은 EMD 서비스 센터 (102)의 기본 기능을 예시하였다. 주로, 도 20에 도시된 것처럼 EMD 센터 (102)는 콘텐츠 제공자 (101) 및 SAMS 105₁에서 105₄에게 라이선스 키 데이터를 제공하고, CER_{SAM4}를 통해서 공개 키 인증 데이터 CER_{CP} 및 CER_{AM1}을 발하고, 키 파일 CF를 생성하고, 사용 로그 데이터 (108)에 기초하여 요금 결산 (profit distribution)을 실행한다.

라이선스 키 데이터의 공급

EMD 서비스 센터 (102)로부터 사용자 홈 네트워크 (103)의 SAMS 105₁에서 105₄에게로 라이선스 키 데이터를 전달하기 위한 프로세스가 먼저 설명된다.

EMD 서비스 센터 (102)는 정해진 기간동안, 예를 들어 3 개월 기준으로 라이선스 키 데이터 KD₁에서 KD₃을 판독하고, EMD 서비스 센터 (102)의 개인 키 데이터 K_{ESC,S}를 사용하여 해쉬 값으로부터 서명 데이터 SIG_{KD1,ESC}로부터 SIG_{KD3,ESC}까지를 생성한다. EMD 서비스 센터 (102)는 그후 세션 키 데이터 K_{SES}를 사용하여 라이선스 키 데이터 KD₁에서 KD₃ 및 서명 데이터 SIG_{KD3,ESC}를 3개월 기준으로 암호화한다. 여기서 세션 키 데이터는 SAMS 105₁에서 105₄까지와 상호 진정성을 확인하여 획득되고, 암호화된 데이터를 SAMS 105₁에서 105₄로 전달한다.

유사하게 EMD 서비스 센터 (102)는 예를 들어 여섯달 동안 라이선스 키 데이터 KD₁에서 KD₆을 콘텐츠 제공자 (101)에게 전달한다.

공개 키 인증 데이터의 공급

EMD 서비스 센터 (102)가 콘텐츠 제공자 (101)로부터 공개 키 인증 데이터 CER_{CP}의 공포를 요구하는 리퀘스트를 수신하였을 때 실행되는 프로세스에 대한 설명이 주어진다.

콘텐츠 제공자 (101)로부터 콘텐츠 제공자 (101) CP_ID 의 식별자, 공개 키 데이터 K_{CP,P} 및 서명 데이터 SIG_{9,CP} 를 수신하였을 때 EMD 서비스 센터(102)는 콘텐츠 제공자 (101)와 상호 진정성을 확인하여 획득된 세션 키 데이터 K_{SES} 를 사용하여 그런 데이터를 암호화해한다.

암호화해된 서명 데이터 SIG_{9,CP} 의 진정성을 검증한 후에 EMD 서비스 센터(102)는 식별자 CP_ID 및 공개 키 데이터 K_{CP,P} 에 기초하여 공개 키 인증 데이터의 공포를 요구받은 콘텐츠 제공자 (101)가 CP 데이터베이스에 레지스터될지의 여부를 결정한다.

그후 EMD 서비스 센터(102)는 인증 데이터베이스로부터 콘텐츠 제공자(101)의 X.509-포맷 공개 키 인증 데이터 CER_{CP} 를 판독하고, EMD 서비스 센터(102)의 개인 키 K_{ESC,S} 를 사용하여 공개 키 인증 데이터 CER_{CP} 의 해위값으로부터 서명 데이터 SIG_{1,ESC} 를 생성한다.

EMD 서비스 센터(102)는 콘텐츠 제공자(101)와 상호 진정성 확인을 실행하여 획득된 세션 키 데이터 K_{SES} 를 사용하여 공개 키 인증 데이터 CER_{CP} 와 서명 데이터 SIG_{1,ESC} 를 암호화하고, 암호화된 데이터를 콘텐츠 제공자(101)로 전달한다.

EMD 서비스 센터(102)가 SAM 105₁로부터 공개 키 인증 데이터 CER_{SAM1} 을 발하라는 리퀘스트를 수신했을 때 실행될 프로세스는 프로세싱이 SAM 105₁에 대해 실행된다는 것을 제외하고는 콘텐츠 제공자(101)로부터 공개 키 인증 데이터 CER_{CP}를 발송하라는 리퀘스트를 수신했을 때의 프로세스와 유사하다. 공개 키 인증 데이터 CER_{SAM1} 은 또한 X.509 포맷으로 설명된다.

본 발명에서 SAM 105₁을 선적(shipping)할 때 개인 키 데이터 K_{SAM1,S} 및 공개 키 데이터 K_{SAM1,P} 가 SAM 105₁의 저장 유닛에 저장되도록 디자인되었다면 EMD 서비스 센터(102)는 SAM 105₁을 선적할 때 공개 키 데이터 K_{SAM1,P}의 공개 키 인증 데이터 CER_{SAM1}을 생성할 수 있다. 이 경우에 생성된 공개 키 인증 데이터 CER_{SAM1}은 SAM 105₁을 선적할 때 SAM 105₁의 저장 유닛에 저장될 수 있다.

키 파일 KF의 생성

콘텐츠 제공자(101)로부터 도 6에 도시된 레지스트레이션 모듈 Mod₂를 수신하였을 때 EMD 서비스 센터(102)는 콘텐츠 제공자 (101)와 상호 진정성 확인을 행한 후에 획득된 세션 키 데이터 K_{SES}를 사용하여 레지스트레이션 모듈 M_{od2}를 디코드한다. EMD 서비스 센터(102)는 그후 키 데이터베이스로부터 판독된 공개 키 데이터 K_{CP,P}를 사용하여 서명 데이터 SIG_{M1,CP}의 진정성을 검증한다.

다음으로, EMD 서비스 센터(102)는 UCP 데이터 (106), 콘텐츠 키 데이터 K_c, 디지털 워터마크 정보 제어 데이터 W_M, 및 레지스트레이션 모듈 Mod₂에 저장된 SRP를 UCP 데이터베이스에 레지스터한다. EMD 서비스 센터(102)는 키 서버에서 판독된 상용 주기 내의 라이선스 키 데이터 KD₁으로부터 KD₆까지를 사용하여 콘텐츠 키 데이터 K_c, UCP 데이터 (106), 및 SAM 프로그램 다운로드 컨테이너 SDC₁으로부터 SDC₃까지를 암호화한다.

EMD 서비스 센터(102)는 그후 자신의 개인 키 데이터 K_{ESC,S}를 사용하여 해디 데이터의 해위 값, 콘텐츠 키 데이터 K_c, UCP 데이터 (106), 및 SAM 프로그램 다운로드 컨테이너 SDC₁에서 SDC₃까지의 것으로부터 서명 데이터 SIG_{K1,ESC}를 생성한다. 이런 방식으로 EMD 서비스 센터(102)는 도 3b에 도시된 키 파일 KF를 생성하고 이를 KF 데이터베이스에 저장한다.

이후, EMD 서비스 센터 (102)는 KF 데이터베이스로부터 키 파일 KF를 판독하고 콘텐츠 제공자 (101)와 상호 진정성을 확인하여 획득된 세션 키 데이터 K_{SES}를 사용하여 이를 암호화하고, 이를 콘텐츠 제공자(101)에게 전달한다.

결산 처리

EMD 서비스 센터(102)에서 실행되는 요금 결산은 다음과 같다.

예를 들어 사용자 홈 네트워크 (103)의 SAM 105₁로부터 사용 로그 데이터 (108) 및 그것의 서명 데이터 SIG_{200,S} AM₁ 을 수신하였을 때 EMD 서비스 센터 (102)는 SAM 105₁와 상호 진정성을 확인하여 획득된 세션 키 데이터 K_S ES 를 사용하여 그런 데이터를 암호해제하고, 이로써 SAM 105₁의 공개 키 데이터 K_{SAM1} 에 의해 생성된 서명 데이터 SIG_{200,SAM1} 을 검증한다.

도 21은 사용 로그 데이터 (108)에 설명된 데이터를 예시하였다. 사용 로그 데이터(108)는 도 21에 예시된 대로, 예를 들어 다음에 기재된 데이터들을 포함한다. EMD 서비스 센터(102)에 의해 제공된 전역적으로 단일화된(globally unique) 식별자이고 보안 컨테이너(104)에 저장된 콘텐츠 데이터 C에 대한 ESC_content ID, 콘텐츠 제공자(101)에 의해 제공된 전역적으로 단일한 식별자이고 콘텐츠 데이터 C에 대한 CP_content ID, 보안 컨테이너 (104)를 수신하였던 사용자의 식별자인 사용자 ID, 사용자 정보, 보안 컨테이너 (104)를 수신한 SAMs 105₁으로부터 105₄까지의 각각의 식별자인 SAM_ID, 상응하는 SAM이 속하는 홈 네트워크 그룹의 식별자인 HNG_ID, 디스카운트 정보, 트레이싱 정보, 가격 프리표, 콘텐츠 데이터 C를 제공하였던 콘텐츠 제공자(101)의 CP_ID, 서비스 제공자(포털)ID, 하드웨어 제공자 ID, 보안 컨테이너(104)를 기록하는 기록 매체 Media_ID의 식별자, 보안 컨테이너(104)의 압축 방법과 같은 지정된 소자의 식별자인 소자 ID, 보안 컨테이너(104)의 라이선스 소유자 LH_ID의 식별자, 및 보안 컨테이너(104)의 요금 결산을 수행하는 EMD 서비스 센터(102) ESC_ID의 식별자.

아래에 설명되는 제 2 실시예에서 사용 로그 데이터(108)에 포함된 상기 설명된 데이터에 부가하여, 사용 로그 데이터 (308)는 콘텐츠 데이터 C에 대해 서비스 제공자(310)가 제공한 식별자 SP_content ID, 및 콘텐츠 데이터 C를 배분했던 서비스 제공자(310) SP_ID의 식별자를 포함한다.

단약 사용자 홈 네트워크(103)의 사용자가 지불한 것이 콘텐츠 제공자(101)와의 권리 보유자, 예를 들어 압축 방법이나 기록매체 등에 대한 라이선스 소유자에게 분배되는 것이 필요하다면 EMD 서비스 센터(102)는 지정된 분배율에 따라서 지불되는 금액을 결정하고 결정된 지불 금액에 기초하여 결산 보고 데이터 및 결산 리퀘스트 데이터 (152)를 생성한다.

이후, EMD 서비스 센터(102)는 SRP, UCP 데이터베이스로부터 판독된 UCP 데이터 (106)에 포함된 할인 가격, 및 사용 로그 데이터 (108)에 기초하여 요금 결산을 수행하고, 결산 리퀘스트 데이터(152) 및 결산 보고 데이터(107)을 생성한다.

결산 리퀘스트 데이터 (152)는 상기 언급한 데이터에 기초하여 결산 조직(91)에 대해 지불을 청구할 수 있는 권한 있는 데이터이고, 단약 사용자가 행한 지불이 다수의 권리 보유자들에게 분배되어야 한다면 결산 리퀘스트 데이터(152)는 각 권리 보유자들에 대해 생성된다.

EMD 서비스 센터(102)는 그후 상호 진정성 확인을 하고 세션 키 데이터 K_{SES} 를 사용하여 결산 리퀘스트 데이터 (152) 및 서명 데이터 SIG₉₉ 을 암호해제하고, 이들을 도 1에 도시된 지불 게이트웨이 (90)를 경유하여 결산 조직(91)으로 전달한다. 따라서, 결산 리퀘스트 데이터(152)에 표시된 지불 금액은 콘텐츠 제공자 (101)에게 지불된다. EMD 서비스 센터(102)는 결산 보고 데이터(107)를 콘텐츠 제공자(101)에게 전달한다.

[사용자 홈 네트워크 103]

도 1에 도시된 대로 사용자 홈 네트워크 (103)는 네트워크 디바이스 (160₁) 및 A/V 머신 (160₂)에서 (160₄)를 포함한다. 네트워크 디바이스 (160₁)은 내장된 SAM (105₁)를 갖는다. A/V 머신 (160₂)에서 (160₄)는 내장된 SAMs (105₂)에서 (105₄)를 구비하였다. SAMs (105₂)에서 (105₄)는 버스(191), 예를 들어 IEEE - 1394 직렬 인터페이스 버스를 경유하여 서로 접속된다.

네트워크 통신 기능은 필수적인 것은 아니지만 A/V 머신 (160₂)에서 (160₄)에게 제공될 수 있다. 네트워크 통신 기능이 제공되지 않는다면 A/V 머신 (160₂)에서 (160₄)는 버스(191)를 경유하여 네트워크 디바이스 (160₁)의 네트워크 통신 기능을 단순히 사용할 수 있다. 대안으로, 사용자 홈 네트워크 (103)는 네트워크 기능 없이 A/V 머신만을 포함할 수 있다.

네트워크 디바이스 (160₁) 의 상세한 설명이 아래에 주어진다.

도 22 는 네트워크 디바이스 (160₁) 의 블록도이다. 네트워크 디바이스 (160₁) 는 SAM (150₁) , 통신 모듈(162), A / V 압축/압축 해제 SAM (163), 작동 유닛 (165), 다운로드 메모리 (167), 플레이백 모듈 (169), 외부 메모리 (201), 및 호스트 중앙 처리 장치(CPU) (810)로 형성된다.

호스트 CPU(810) 는 네트워크 디바이스 (160₁) 내에서 실행되는 처리를 중앙에서 통제하고, 호스트 CPU(810) 및 SAM (105₁) 은 주종 관계를 갖는다. 호스트 CPU (810) 및 SAM (105₁) 사이의 관계는 도 23 을 참조하여 아래에 자세히 설명된다.

도 23 에 도시된 네트워크 디바이스(160₁) 에서 호스트 CPU (810) 및 SAM (105₁) 는 호스트 CPU 버스(1000) 을 공유하여 접속된다. 다수의 인터럽트 타입 중 하나가 사용자에 의해 작동 유닛(165)에서 실행된 작동에 따라서 선택되었다면 호스트 CPU(810)는 선택된 인터럽트를 표시하는 외부 인터럽트(하드웨어 인터럽트) S165 를 수신한다.

인터럽트 S165 에 상응하는 작업이 SAM (105₁) 에 의해 실행되는 것이 발견되었다면 호스트 CPU(810)는 호스트 CPU 버스(1000)를 공유하여 작업을 표시하는 내부 인터럽트(소프트웨어 인터럽트) S810 을 출력한다.

그러면 SAM (105₁) 는 호스트 CPU (810)에 의해서 입력/출력(I/O) 디바이스로서 인식되고, 호스트 CPU(810)으로 부터 기능 콜(function call)인 내부 인터럽트 S810 을 수신하였을 때 SAM (105₁)은 요구된 작업을 실행하고 실행 결과를 호스트 CPU (810)에게 리턴한다.

SAM(105₁)에 의해 실행되는 주요 작업들은 콘텐츠 데이터 (계산 프로세싱)의 취득, 서명 체크, 상호 인증, 콘텐츠 데이터의 재생, 업데이팅, 등록, 다운로드 등을 위한 프로세싱을 포함할 수 있다. 이러한 작업들은, 외부 소스로부터 완전히 보호되면서 SAM(105₁) 내에서 처리되고, 이에 의해서 호스트 CPU(810)가 처리된 결과를 모니터링하는 것을 방지한다.

호스트 CPU(810)는 이벤트의 타입에 따라 SAM(105₁)에 작업들이 요청되었다는 것을 알고 있다. 보다 상세하게는, 동작 유닛(165) 상에서 행해진 사용자의 동작에 의한 외부 인터럽트(S165)를 수신하면, 호스트 CPU(810)는 외부 인터럽트(S165)에 의한 작업이 SAM(105₁)에 의해 실행된다는 것을 결정한다. 그 다음, 호스트 CPU(810)는 호스트 CPU 버스(1000)를 통해 SAM(105₁)으로 내부 인터럽트(S810)를 출력하여, 이것이 작업을 실행하도록 요청하게 한다.

외부 키 디바이스, 예를 들어 커맨드나 키보드와 같은, I/O 디바이스로부터 호스트 CPU(810)로의 인터럽트들은 호스트 CPU(810)에 의해 실행되는 사용자 프로그램과 비동기적으로 발생한다. 이러한 인터럽트들은 보통은 " 하드웨어 인터럽트들" 또는 " 외부 인터럽트들" 로 언급된다.

콘텐츠를 보고 듣고 또한 이 콘텐츠를 취득하기 위해, 호스트 CPU(810)에 의해 수신된 인터럽트들이 하드웨어 인터럽트들이다. 이 경우, 하드웨어 인터럽트들을 발생하는 I/O 디바이스는, 네트워크 디바이스(160₁)의 버튼 또는 그래픽 사용자 인터페이스(GUI) 아이콘과 같은, 키 디바이스일 수 있다. 본 실시예에서는, 동작 유닛(165)이 이러한 I/O 디바이스로서 작용한다.

한편, 호스트 CPU(810)에 의한 사용자 프로그램 (프로그램) 실행에 의해 발생된 인터럽트들은 " 소프트웨어 인터럽트들" 또는 " 내부 인터럽트들" 로서 참조된다.

일반적으로, 외부 인터럽트(S165)의 인터럽트 신호는, 호스트 CPU 버스(1000)로부터 개별적으로 제공되는, 외부 인터럽트용 특정 라인을 통해 동작 유닛(165)으로부터 호스트 CPU(810)로 출력된다.

한 외부 인터럽트(S165)는, 인터럽트를 발생하는 I/O 디바이스들에 번호를 할당함으로써 다른 외부 인터럽트들(S165)과 구별된다. 예를 들면, 키보드에 대하여, 개개의 버튼에 번호 (이러한 번호를 " 인터럽트 타입" 이라 함)을 할당한다

다. 버튼들 중 하나를 누르면, 대응하는 정보가 특정 라인을 통해 동작 유닛(165)으로부터 호스트 CPU(810)로 보고 되고, 눌러진 버튼의 번호가 I/O 인터페이스의 메모리에 기억된다. 버튼이 눌러졌다는 것을 나타내는 정보에 응답하여, 호스트 CPU(810)는 I/O 인터페이스의 메모리를 액세스하고, 이 버튼의 번호로부터의 인터럽트 타입을 확인하며, 이에 의해 버튼의 번호에 대응하는 인터럽트 루틴의 실행을 제어한다.

이 경우, 인터럽트 루틴이 SAM(105₁)에 의해 실행된다면, 호스트 CPU(810)는 내부 인터럽트(S810)를 SAM(105₁)으로 송신하여 이것이 작업을 실행하도록 요구한다.

상술한 바와 같이, SAM(105₁)에 의해 실행되는 작업들은 다음을 포함한다.

1. 취득 키 및 콘텐츠의 데몬스트레이션을 포함한 콘텐츠의 취득;
2. 콘텐츠의 재생; 및
3. 콘텐츠 제공자(101)와 EMD 서비스 센터(102)로부터의 다운로드 (업데이팅, 사용 로그 수신 및 프로그램 다운로드)

호스트 CPU(810)는 먼저 특정 라인을 통해 동작 유닛(165)으로부터 작업 1, 2 및 3에 대응하는 외부 인터럽트들(S 165)을 수신하고, 그에 대응하는 내부 인터럽트(S810)를 SAM(105₁)으로 출력하여, SAM(105₁)에게 작업 1, 2 및 3을 실행하게 한다.

작업 1 및 2에 대응하는 인터럽트들을 발생하는 I/O 디바이스들은 네트워크 디바이스(160₁)의 버튼이나 GUI와 같은, 외부 키 디바이스이다.

작업 3의 경우, 누름형 다운로드 시큐어 컨테이너(104)가 콘텐츠 제공자(101)로부터 전송되는 것이 아니라, 능동적인 당김형(active pull-type) 시큐어 컨테이너(104)가 콘텐츠 제공자(101)를 액세스하기 위해 폴링(polling)을 수행함으로써 네트워크 디바이스(160₁) (클라이언트)로 전송되는 것이다. 따라서, 호스트 CPU(810)는 다운로드된 시큐어 컨테이너(104)가 네트워크 디바이스(160₁) 내의 다운로드 메모리(167)에 기억된다는 것을 알고 있다. 따라서, 실제로, 호스트 CPU(810)는 단지 내부 인터럽트(S810)를 발생하여, 이것을, 동작 유닛(165)으로부터 외부 인터럽트(S 165)를 수신하지 않고, SAM(105₁)으로 전송한다.

SAM(105₁)은 호스트 CPU(810)의 I/O 디바이스 (슬리브)로서 동작하기 때문에, SAM(105₁)의 메인 루틴은 전원 이 공급될 때 시작된 후, 스탠바이 (대기) 모드로 들어간다.

그 후에, 호스트 CPU(810) (마스터)로부터 내부 인터럽트(S810)를 수신한 직후, SAM(105₁)은 외부 소스로부터 완전 보호하면서, 상기 작업을 처리하기 시작한다. 그 다음 SAM(105₁)은 외부 인터럽트 (하드웨어 인터럽트)에 의해 작업 처리 완료를 호스트 CPU(810)로 보고하여, 호스트 CPU(810)에게 그 결과를 수신하도록 요구한다. 따라서, SAM(105₁)은 사용자 메인 프로그램 (사용자 프로그램)을 포함하지는 않는다.

SAM(105₁)은 콘텐츠의 취득, 상기 콘텐츠의 재생, 및 콘텐츠 제공자(101)와 EMD 서비스 센터(102)로부터의 다운로드 및 같은 프로세싱을 인터럽트 루틴으로서 실행한다. SAM(105₁)은 일반적으로 스탠바이 모드에서 대기하고, 호스트 CPU(810)로부터 내부 인터럽트(S810)를 수신하면, SAM(105₁)은 인터럽트 타입(번호) (기능 호출 커맨드)에 대응하는 인터럽트 루틴을 실행하여 호스트 CPU(810)에게 그 결과를 수신하도록 요청한다.

보다 상세하게는, 내부 인터럽트(S810)에 의한 호스트 CPU(810)로부터 SAM(105₁)으로의 작업을 실행하라는 요구가 I/O 커맨드에 따라 행해지고, 그 다음 SAM(105₁)은 호스트 CPU(810)로부터 수신된 기능 호출 커맨드에 기초하여 그 자신을 인터럽트한다. 실제로, 호스트 CPU(810)는 SAM(105₁)을 선택하기 위한 집 선택을 수행함으로써 내부 인터럽트(S810)를 SAM(105₁)로 출력한다.

상술한 바와 같이, 호스트 CPU(810)는 콘텐츠를 취득 또는 재생하기 위해 외부 인터럽트(S165)를 수신하더라도, 이는 SAM(105₁)에게 대응하는 작업을 실행하라고 요구한다. 이는 작업이 키를 취득하기 위한 프로세싱에 의해 수반되는, 서명들의 암호화 프로세싱, 작성 및 검사를 행하는 것과 같은 기밀 보호와 관련이 있기 때문이다.

SAM(105₁) 내에 기억된 인터럽트 루틴은 호스트 CPU(810)의 인터럽트 루틴의 서브루틴으로서 작용한다.

호스트 CPU(810)에 의해 실행되는 인터럽트 루틴은, 외부 인터럽트(S165)에 대응하는 작업의 실행을 요청하는 내부 인터럽트(기능 호출)(S810)가 SAM(105₁)의 공동 메모리 공간으로 송신하라는 명령을 만드는 작업이다.

도 24에 도시된 바와 같이, SAM(105₁) 내에 기억된 각각의 인터럽트 루틴들은 서브 루틴들을 포함한다. 다른 인터럽트 루틴들로 분할될 수 있는 프로그램들은 바람직하게는 서브루틴들로 규정되며, 이에 의해 메모리 공간을 절약한다. SAM(105₁)의 프로세싱은 인터럽트 루틴으로부터 서브 루틴들을 동시에 규정하거나 제1 발생 서브루틴으로부터 제2 발생 서브루틴을 규정할 수 있도록, CPU에 의해 실행되는 것과 유사한 방법으로 실행될 수 있다.

다시 도 23을 참조하여, 호스트 CPU(810)와 SAM(105₁)의 관계를 설명한다. 상술된 바와 같이, 호스트 CPU(810)는 특정 라인을 통해 외부 인터럽트(하드웨어 인터럽트)(S165)로서, 외부 키 디바이스와 같은 I/O 디바이스로부터의 인터럽트를 수신한다.

각각의 특정 라인에 대해서는 번호가 제공되고, 이 번호에 따라, 대응하는 인터럽트 벡터가 호스트 CPU(810)의 시스템 메모리에 기억된 인터럽트 벡터 표로부터 추출되며, 이에 의해 인터럽트 루틴을 개시한다.

벡터 표에서 인터럽트 벡터의 선택된 번호를 가리키는 간접 액세스 타입 및 인터럽트 루틴의 시작 어드레스를 가리키는 직접 액세스의, 2 종류의 인터럽트 타입이 존재한다.

수신된 외부 인터럽트가 SAM(105₁)에 의해 실행하고자 하는 작업을 가리키면, 호스트 CPU(810)는 내부 인터럽트(S810)를 SAM(105₁)로 출력하여 이 SAM(105₁)에게 작업(I/O 커맨드)을 실행하도록 요구한다.

이러한 타입의 작업은 커맨드 명칭에 의해 규정되고, 호스트 CPU(810)는 커맨드 - 기반 내부 인터럽트(S810)를 SAM(105₁)으로 출력한다. 전원이 공급되면, SAM(105₁)은 프로그램을 시작하여 도 24에 도시된 바와 같이 SAM(105₁)의 완전성을 검사한 다음, 경지 모드(스탠바이 모드)로 들어간다. 이 경지 모드에서는, CPU의 동작만이 정지하고, 경지 모드는 임의의 인터럽트에 의해 해제된다. 그 후, SAM(105₁)의 상태는 실행 조정 상태를 통해 프로그램 실행 상태로 이동된다. 호스트 CPU(810)로부터 내부 인터럽트를 수신할 때, SAM(105₁)은 대응하는 작업을 실행하여 그 결과를 호스트 CPU(810)로 전달한다.

SAM(105₁)으로부터의 결과에 응답하여, 호스트 CPU(810)는 다른 동작을 행하기 시작한다. 그러나, SAM(105₁)이 하나의 작업을 실행 중인 경우에도, 호스트 CPU(810)는 다른 작업을 수행할 수 있다. 호스트 CPU(810)는 인터럽트로서 SAM(105₁)로부터 작업 실행 결과를 수신한다.

SAM(105₁)으로부터의 작업의 실행 결과를 호스트 CPU(810)로 보고하기 위한 2가지 방법이 있다. 한 방법은 호스트 CPU(810)로 인터럽트를 출력하여 호스트 CPU(810)에게 그 결과를 수신하도록 요청하는 것이다. 다른 방법은 호스트 CPU(810)에 의해 액세스 가능한 SAM(105₁)의 어드레스 공간에 ("SAM 상태 레지스터"로 언급됨) 상태 레지스터를 제공하는 것이다. (호스트 CPU(810)로부터의 판독/기입 커맨드, 어드레스 정보 및 데이터는 어드레스 공간으로 전달된다.) 상기 두 번째 방법에 따르면, 작업의 타입, 작업이 대기, 실행 또는 완성되었는지의 여부를 가리키는 플래그들 등이 SAM 상태 레지스터(SAM_SR)에서 설정될 수 있고, 호스트 CPU(810)는 SAM 상태 레지스터로의 폴링(데이터 판독)을 정기적으로 수행한다.

제1 SAM 상태 레지스터는 호스트 CPU(810)에 의해 판독된 SAM(105₁)의 상태를 가리키는 플래그를 설정한다.

제2 SAM 상태 레지스터는 호스트 CPU(810)로부터의 작업 실행이 요구되었는지의 여부를 계획하는 플래그들을 설정한다. 이들 플래그들은 SAM(105₁) 내의 CPU에 의해 판독된다. 버스 중개의 우선 순위에 기초하여, 호스트 CPU(810)와 SAM(105₁)은 모두 제1 및 제2 SAM 상태 레지스터 내에 설정된 플래그들을 액세스가능하게 된다.

보다 상세하게는, 제1 SAM 상태 레지스터에서, 플래그들은 SAM이 작업을 실행중인지, 작업을 완료했는지 또는 실행될 작업을 기다리고 있는지의 여부를 나타내는 플래그를 설정한다. 제1 SAM 상태 레지스터 내에 또한 작업의 명칭을 나타낸다. 호스트 CPU(810)는 정기적으로 폴링을 행하여 제1 SAM 상태 레지스터를 액세스한다.

제2 SAM 상태 레지스터에서는, 작업 실행이 호스트 CPU(810)로부터 요청되었는지 또는 스탠바이 모드 상태에 있는지의 여부를 나타내는 플래그를 설정한다.

I/O 기입 커맨드가 먼저 호스트 CPU(810)로부터, I/O 디바이스인 SAM(105₁)으로 전송되고, 이어서 기입될 데이터와 어드레스 정보가 전송된다. 어드레스 정보 (데이터 기억 위치)는 호스트 CPU(810)와 SAM(105₁)에 의해 분할되는 공동 메모리 공간에 기억된다.

SAM(105₁) 내의 메모리 어드레스 공간은 호스트 CPU(810)로부터 가시적으로 확인할 수 없게 할 필요가 있다 (부정 조작 방지 특성). 따라서, SAM(105₁) 내의 메모리 어드레스 공간은 작업 축적을 위해 정적 랜덤 액세스 메모리 (SRAM)의 일부만이 또는 외부 플래시 ROM [전기적으로 소거가능한 프로그램가능 판독 전용 메모리 (EEPROM)]의 일부만이 호스트 CPU(810)로부터 가시적으로 확인가능하도록 관리된다. 따라서, 대용량 데이터가 호스트 CPU(810)로부터 SRAM의 일부 또는 EEPROM의 일부 안에 기입되고, 저용량 데이터는 호스트 CPU(810)로부터 가시적으로 확인할 수 있는 SAM(105₁) 내의 임시 레지스터 안에 기입된다.

인터럽트에 의해 실행하고자 하는 인터럽트 루틴의 어드레스는 "인터럽트 벡터"로서 참조된다. 인터럽트 벡터는 인터럽트 타입들의 순서에 따라 벡터 표에 기억된다.

도 25에 도시된 바와 같이, 인터럽트 타입 (번호)에 따라 외부 인터럽트를 수신하면, 호스트 CPU(810)는 메모리에 기억된 인터럽트 벡터 표로부터 인터럽트 벡터를 추출하여, 그 어드레스 (인터럽트 벡터)로부터 시작된 대응하는 루틴을 서브루틴으로서 실행한다.

본 실시예에서, 상술한 작업 1 내지 3중 하나를 수행할 때, 대응하는 I/O 디바이스로부터 물리적인 인터럽트 신호에 의해 외부 인터럽트가 발생하고, 호스트 CPU(810)는 내부 인터럽트 (소프트웨어 인터럽트)를 사용하여 기능 호출 (진행 호출)을 SAM(105₁)으로 송신하여, 이 SAM(105₁)에게 인터럽트 타입 (번호)에 따라 인터럽트 루틴 (작업)을 실행하도록 요구한다. 그 다음, 호스트 CPU(810)는 작업 실행 결과를 수신하여 다른 동작을 취하기 시작한다.

상기 내부 인터럽트는 도 26에 도시된 바와 같이, 사용자 프로그램, 즉 CPU로부터 발생된 소프트웨어 인터럽트이다. 이 내부 인터럽트는 기계언어로 된 INT 커맨드의 실행에 의해 발생된다.

다음은 기능 호출 (진행 호출)에 대한 상세한 설명이 이어진다.

인터럽트 루틴은 작은 기능들로 형성되고, 커맨드 명칭은 각각의 기능에 대해 규정된다. 사용자 프로그램으로부터 인터럽트 커맨드 INT와 함께 커맨드 명칭을 계획함으로써, 타겟 기능이 완료될 수 있다. 이를 "기능 호출 (진행 호출)"로서 참조한다. 이러한 방법에서, 기능 호출은 내부 인터럽트 (소프트웨어 인터럽트)를 통해 수행된다.

함수 호출을 할 때, 인터럽트 루틴을 실행하기 위한 파라미터가 CPU의 레지스터 내에 기능 호출 번호를 입력함으로써 전달됨으로써, 타겟 함수를 지정한다. 결과는 레지스터 또는 메모리로 되돌아가거나, 대응하는 동작이 행해진다.

예를 들면, 도 27에 도시된 유저 프로그램 내의 코드 A를 실행할 때, 호스트 CPU(810)는 인터럽트 명령 INT 및 명령 이름을 지정하고, SAM(1051)의 CPU는 인터럽트 타입에 대응하는 메모리 영역을 액세스하고, 또한 명령 분석기에 액세스함으로써, 함수 3의 서브루틴을 실행한다.

SAM(1051)의 CPU의 프로세싱 상태는 도 28을 참조하여 후술한다.

도 28에 도시된 바와 같이, SAM(1051)의 CPU에는 5가지 상태가 있는데, 리셋 상태 ST1, 예외 핸들링 상태 ST2, 프로그램 실행 상태 ST3, 버스 우측 해제 (bus right release) 상태 ST4, 및 저전력 상태 ST5가 있다.

개별적인 상태에 대한 세부 사항은 다음과 같다.

리셋 상태 ST1은 CPU가 리셋된 상태이다.

예외 핸들링 상태 ST2는 CPU가 리셋팅 또는 인터럽트 프로세싱 등과 같은 외부적인 핸들링 요인에 의해 프로세싱 상태를 쉬프트시키는 현이 상태이다. 인터럽트 프로세싱을 행할 때, 스택 포인터 (SP)를 참조함으로써, 프로그램 카운터 (PC)의 카운트값 및 상태 레지스터(SR)의 값이 스택 영역에 임시로 기억된다. 그 다음, 인터럽트 루틴이 시작되는 어드레스가 예외 핸들링 벡터표로부터 추출되고, 루틴은 어드레스로 분기됨으로써, 프로그램을 시작한다. CPU의 상태는 프로그램 실행 상태 ST3로 쉬프트한다.

프로그램 실행 상태 ST3은 CPU가 순차적으로 프로그램을 실행하고 있는 상태이다.

버스 우측 해제 상태 ST4는 CPU가 버스 우측을 요구한 장치에 대하여 버스를 해제하는 상태이다.

저전력 상태 ST5는 슬립 모드(sleep mode), 스탠바이 모드, 및 모뎀 스탠바이 모드 등의 3가지 모드를 갖는다.

(1) 슬립 모드

CPU의 동작은 계속되지 않으나, CPU의 내부 레지스터에 기억된 데이터, 내장된 캐쉬 메모리 내의 데이터, 및 내장용 RAM 내의 데이터는 보유된다. CPU를 제외한 내장된 주변 모듈의 기능은 여전히 작동하고 있다.

슬립 모드는 임의의 인터럽트, 또는 직접 메모리 액세스 (DMA) 에러를 리셋팅함으로써 해제되고, 예외 핸들링 상태 ST2를 통해 프로그램 실행 상태 ST3로 쉬프트한다.

(2) 스탠바이 모드

스탠바이 모드에서는, CPU, 내장 모듈, 및 발전기의 기능이 완전히 정지된다. 내장용 캐쉬 메모리의 데이터 및 내장용 RAM의 데이터는 보유되지 않는다. 스탠바이 모드는 리셋팅 또는 외부 마스크불가능 인터럽트 (NMI)에 의해 해제된다. 해제된 다음, 스탠바이 모드가 발전을 안정화하는데 필요한 시간이 경과한 후에, 예외 핸들링 상태 ST2를 통해 정규 프로그램 상태로 쉬프트한다. 스탠바이 모드에서는, 발전기가 정지되어 있기 때문에, 전력 소비가 상당히 감소된다.

(3) 모뎀 스탠바이 모드

DMA 등의 내장용 모듈로의 클럭 공급은 계속되지 않는다.

호스트 CPU(810)와 SAM(1051)과의 관계는 도 29를 참조하여 메모리 공간을 통해 후술된다.

도 29에 도시된 바와 같이, 유저의 조작을 통해 외부 인터럽트를 수신하면, 호스트 CPU(810)이 CPU(810a)가 유저 프로그램의 실행을 인터럽트하고, 인터럽트 타이밍을 지정하여 인터럽트 벡터 표의 하드웨어 인터럽트 영역을 액세스한다. 그 다음, CPU(810a)는 액세스된 어드레스 내에 저장된 인터럽트 루틴을 실행한다. 인터럽트 루틴은 내부 인터럽트인 함수 호출 1-1, 1-2, 2, 또는 3을 SAM(1051)에 출력하여 SAM(1051)에 해당 작업을 실행할 것을 요구하고, SAM(1051)으로부터의 실행 결과를 얻은 다음, 유저 프로그램으로 복귀하는 프로세스에 대해 설명한다. 보다 구체적으로는, CPU(810a)는 작업을 특정하는 정보를 SAM(1051) 내의 메모리(1051)의 일부를 형성하고 호스트 CPU(810) 및 SAM(1051)의 공통 메모리로서 역할을 하는 SRAM(1155)에 기록한다.

내부 인터럽트를 SAM(1051)에 출력할 때, 호스트 CPU(810)의 CPU(810a)는 SAM(1051) 내의 제2 SAM 상태 레지스터(1156b)의 작업 대기 플래그를 턴 온한다.

SAM(1051)의 CPU(1100)는 제2 SAM 상태 레지스터(1156b)를 점검하고 SRAM(1155)에 액세스하여 호스트 CPU(810)에 의해 요구된 작업의 타입을 특정함으로써, 대응하는 인터럽트 루틴을 실행한다. 인터럽트 루틴은, 상술한 바와 같이, 예를 들면, 기록 매체, A/V 압축/압축 해제 SAM, 미디어 드라이브 SAM, IC 카드, 및 EMD 서비스 센터(102)와의 상호 인증, 기기들 간의 상호 인증을 포함하는 서브 루틴을 판독하고, 서명 데이터를 생성하고 점검함으로써 실행된다.

SAM(1051)의 CPU(1100)는 SRAM(1155)에 인터럽트 루틴의 결과(작업 결과)를 저장하고, 또한 SAM(1051) 내의 제1 SAM 상태 레지스터(1156a)의 작업 종료 플래그를 턴온한다.

제1 SAM 상태 레지스터(1156a)의 작업 종료 플래그가 온 된 것을 점검한 후에, 호스트 CPU(810)는 SRAM(1155)으로부터 작업 결과를 판독하고 유저 프로그램의 프로세싱으로 되돌아간다.

SAM(1051)의 기능은 다음과 같다. SAM(1052) 내지 SAM(1054)의 기능은 SAM(1051)과 유사하다.

SAM(1051)은 각 콘텐츠에 대한 어카운팅 프로세싱을 행하고, EMD 서비스 센터(102)와 통신한다. SAM(1051)의 규격 및 버전은 EMD 서비스 센터(102)에 의해 관리될 수 있다. 가정용 전자 기기 제조업자에 의해 SAM(1051)이 가정용 전자 기기에 적용하는 것이 바람직한 경우, EMD 서비스 센터(102)는 이러한 제조업자에게 자격을 부여하여 콘텐츠 단위로 어카운팅하기 위한 블랙 박스 어카운팅 모듈로서 SAM(1051)을 사용할 수 있다. 예를 들면, EMD 서비스 센터(102)는 제조업자에게 알리지 않고 SAM(1051)의 IC 인터페이스 등의 IC를 규격화하고, SAM(1051)은 규격에 따라서 네트워크 장치(1601) 내에 로딩된다. SAM(1052) 내지 SAM(1054)은 A/V 기기(1602 내지 1604)를 통해 A/V 기기(1602)에 각각 로딩된다.

SAM(1051)의 프로세싱 콘텐츠는 외부원으로부터 완전히 차폐되고 따라서 외부에서 모니터링하여 변경하는 것이 보호된다. SAM(1051)은 사전에 저장된 데이터나 현재 처리중인 데이터가 변경될 수 없는 변경 방지 하드웨어 모듈(예를 들면, IC 모듈)을 실행시키거나, CPU에 의해 소프트웨어(전용 프로그램)를 실행시킴으로써 구현되는 기능 모듈이다.

SAM 1051의 기능이 IC에 의해 구현되면, 전용 메모리는 IC 내에 배치되고, 전용 프로그램 및 전용 데이터는 개인 메모리에 저장된다. SAM(1051)의 기능이 IC 등의 물리적 형태를 이용하여 구현되기보다는 기계의 일부로 통합되면, 기능들을 통합하는 부분이 SAM으로서 정해질 수 있다.

도 22에 도시된 네트워크 장치(1601)의 예에서는, 시큐어 컨테이너(104)가, 실제로 표시한 바와 같이, 통신 모듈(162)에서 SAM(1051)으로 출력된다. 그러나, 점선 체인으로 표시한 바와 같이, 키 파일 KF가 통신 모듈(162)로부터 SAM(1051)으로 출력될 수 있고, 콘텐츠 파일 CF가 CPU 버스를 통해 통신 모듈(162)로부터 다운로드 메모리(167)로 직접 기록될 수 있다.

콘텐츠 데이터 C는 SAM(1051)을 스킵함으로써 다운로드 메모리(167)로부터 직접 A/V 압축/압축 해제 SAM(163)에 출력될 수 있다.

SAM(1051)의 기능은 도 30의 기능적 블록을 참조하여 이하에 구체적으로 설명한다.

도 30은 콘텐츠 프로바이더(101)로부터 보안 컨테이너(104)를 수신하고 이 보안 컨테이너(104) 내의 키 파일(KF)을 암호해제하는 처리를 위한 데이터 흐름을 나타낸다.

그 후, 단계 S55-11에서, 보안 컨테이너(104y) 내의 키 파일 KF 및 서명 데이터 SIG_{7,CP} 및 SIG_{350,SAM3} 와, 공개 키 증명 데이터 CER_{CP} 및 서명 데이터 SIG_{351,ESC} 와, 공개 키 증명 데이터 CER_{CP} 및 서명 데이터 SIG_{1,ESC} 가 작업 메모리(200)로 기입된다.

단계 S55 - 12에서, SAM(105)의 서명 프로세서(189)가 보안 컨테이너(104y) 즉, 생성기(creator)와 콘텐츠 파일 CF의 송신기(sender)와의 통합에 저장된 서명 데이터 SIG_{6,CF} 및 SIG_{390,SAM}를 증명한다.

그 후, 단계 S55 - 13에서, 콘텐츠 파일 CF는 호스트 CPU(810)의 제어하에 SAM(105) 없이, 매체 드라이브 SAM 관리자(855)를 지나 기록 매체(RAM) (130)의 RAM 영역(134)으로 직접 기입될 수 있다.

그 후, 단계 S55 - 14에서, 서명 프로세서(189)는 서명 데이터 SIG_{391,ECS}의 서명을 체크하여서, 공개 키 증명 데이터 CER_{SAM}의 통합성(integrity)을 증명하고, 그 후 공개 키 증명 데이터 CER_{SAM}에 저장된 공개 키 데이터 K_{SAM} 및 공개 키 데이터 K_{ESC}를 사용하여, 서명 데이터 SIG_{7,CF}, SIG_{392,SAM}, 및 SIG_{8,ESC}와의 통합, 즉 생성기와 키 파일 KF의 송신기와의 통합을 증명한다.

그 후, 단계 S55 - 15에서, 키 파일 KF가 작업 메모리(200)에서 암호/암호해제(디코딩) 유닛(172)으로 판독되고, 허가(license) 키 데이터 KD 내지 KD_i를 이용하여 디코딩되고, 작업 메모리(200)로 다시 기입된다.

단계 S55 - 16에서, 작업 메모리(200)에 저장된 디코딩된 키 파일 KF의 UCP 데이터(106)가 사용(usage) 모니터(186)로 출력된다. 그 후, 구입 모드 및 사용 모드는 UCP 데이터(106)에 기초되어 사용 모니터(186)에서 관리된다(모니터링됨).

단계 S55 - 17에서, 도 52에 도시된 동작 유닛(165)상의 사용자의 동작에 의해, 콘텐츠의 구매 및 사용 모드들이 결정되고, 해당하는 내부 인터럽트(S810)가 SAM(105)의 CPU(1100)로 출력된다.

단계 S55 - 18에서, UCS 데이터(166) 및 사용 로그 데이터(108)가 결정된 구매 및 사용 모드들에 기초되어 계산(ac counting) 프로세서(187)에서 생성되고, 작업 메모리(200)와 외부 메모리(201)로 각각 기입된다. UCS 데이터(166) 및 사용 로그 데이터(108)는 EMD 서비스 센터(102)로 적절하게 전송된다.

그 후, 단계 S55 - 19에서, 콘텐츠 키 K_c 및 UCS 데이터(166)가 작업 메모리(200)로부터 암호/암호해제(디코딩) 유닛(173)으로 판독되고, 저장 유닛(192)으로부터 판독된 저장 키 데이터 K_{STR}, 매체 키 데이터 K_{MEDQ}, 및 구매자 키 데이터 K_{PIN}을 사용함으로써 순차적으로 암호화된다. 그 후, 암호화된 데이터는 매체 SAM 관리자(197)로 출력된다. 키 파일 KF는 또한, 작업 메모리(200)로부터 매체 SAM 관리자(197)로 출력된다.

단계 S55 - 20에서, 도 44C에 도시된 키 파일 KF₁은 매체 SAM 관리자(197)에서 생성되고, 매체 SAM 관리자(197)를 지나 기록 매체 (RAM) (130)의 매체 SAM(133)으로 기입된다. 키 파일 KF는 또한, 매체 SAM 관리자(197)를 지나 기록 매체 (RAM) (130)의 매체 SAM(133)에 기입된다.

단계 S55 - 21에서, SAM(105)의 CPU(1100)는 상술된 처리가 정확히 행해졌는지를 판정하고, 그 결과를 외부 인터럽트를 통해 호스트 CPU(810)에 보고한다.

또 다른 방법으로, CPU(1100)는 상술된 처리가 정확히 행해졌는지를 가리키는 SAM 상태 레지스터에 플래그를 설정할 수 있으며, 호스트 CPU(810)는 폴링(polling)에 의해 플래그를 판독할 수 있다.

SAM(105,내지105)의 구현 방법이 다음과 같이 설명된다.

SAM(105,내지105)의 기능들을 하드웨어로서 구현하기 위해, 내장(built-in) 메모리를 갖는 애플리케이션 스펙트화된 IC(ASIC) - 타입 CPU가 사용되고, 보안 기능 모듈, 콘텐츠 권리(right) 처리를 행하기 위한 프로그램 모듈, 및 키 데이터와 같은 고도의 보안 데이터가 메모리에 저장되어, 도 30에 도시된 기능들을 구현할 수 있다. 암호 라이브러리(library) 모듈과 같은 일련의 권리 처리 프로그램 모듈들(공개 키 암호화, 공통 키 암호화, 랜덤한 번호 발생기, 해쉬 함수), 콘텐츠의 사용을 제한하기 위한 프로그램 모듈, 계산 프로그램 모듈 등이 예를 들어, 소프트웨어로서 구현된다.

예를 들어, 암호/암호해제(디코딩) 유닛(171)과 같은 모듈이 처리 속도의 관점에서는 하드웨어로서 ASIC - 타입 CPU 내의 IP 코어로 구현된다. 클럭 속도 또는 CPU 코드 시스템과 같은 성능면에서는 암호/암호해제(디코딩) 유닛(171)이 소프트웨어로서 구현될 수 있다.

프로그램 모듈을 저장하기 위한 저장 유닛(192) 및 메모리와, 도 30에 도시된 기능들을 구현하기 위한 데이터로서, 비-휘발성 메모리(플래시 ROM)가 사용될 수 있으며, SRAM과 같은 고속 메모리가 작업 메모리로서 사용될 수 있다. 또는, FeRAM이 SAM(105,내지105)에 집적된 메모리로서 채택될 수 있다.

SAM(105,내지105)은 또한, 콘텐츠의 사용을 위한 유효 기간 및 계약 기간을 증명하기 위해 필요되는 시간 및 날짜를 체크하기 위해, 내장된 타이밍 기능을 갖는다.

상술된 바와 같이, SAM(105,내지105)은 프로그램 모듈, 데이터, 및 처리 콘텐츠들이 외부 소스로부터 보호되는 부정 변경이 매우 어려운 구조를 갖는다. 각 SAM은 호스트 CPU의 메모리 어드레스를 관리하기 위한 메모리 관리 유닛(MMU)을 사용함으로써, 해당 호스트 CPU로부터는 나타나지 않는 어드레스 공간을 설정한다. 이러한 구성을 갖고, 각 SAM의 IC 메모리에 저장된 매우 은밀한 프로그램 및 데이터의 콘텐츠와, SAM의 시스템 구성에 관련된 레지스터 그룹과, 암호 라이브러리와 클럭 레지스터 그룹이 호스트 CPU 버스를 통해 관독되거나 기입되는 것으로부터 보호될 수 있다. 즉, 상술된 각 SAM의 데이터 및 프로그램들은 호스트 CPU에 의해 할당된 어드레스 공간에 존재하지 않도록 보호된다.

SAM(105,내지105)은 또는, X 선 및 열과 같은 외부 소스로부터의 물리적 공격에 저항력을 갖는다. 또한, 디버깅 불(hardware in-circuit emulator; ICE) 또는 소프트웨어 ICE)을 사용함으로써 실시간 디버깅(역처리(reverse engineering))이 행해진다해도, 처리 콘텐츠가 보이지 않거나, 또는 디버깅 불 그 자체가 IC를 제조한 후에는 소용없어진다.

하드웨어 구조면에서, SAM(105,내지105)은 내장된 메모리를 갖는 레귤러 ASIC0타입 CPU이며, SAM(105,내지105)은 CPU를 동작시키는 소프트웨어에 따라 변화한다. 그러나, SAM(105,내지105)은, SAM(105,내지105)이 암호 기능이 제공되고 부정 변경이 어려운 하드웨어 구조를 가졌다는 점에서 레귤러 ASIC - 타입 CPU와는 다르다.

한편, 소프트웨어로서 SAM(105_{1} 내지 105_{j})의 모든 기능들을 구현하는 데에는 2가지 방법이 있다. 한 방법은 부정 변경이 매우 어려운 완전 차폐된 모듈내에서 소프트웨어 처리를 행하는 것이다. 다른 방법은 통상의 기계에 설치된 호스트 CPU에서 소프트웨어 처리를 행하는 것으로, 소프트웨어 처리는 디코딩하기에 매우 어렵다. 첫번째 방법에서, 암호 라이브러리 모듈이 지적 재산(IP) 코어보다는 레귤러 소프트웨어 모듈로서 메모리에 저장되는 즉, 하드웨어로서 구현되는 것이 고려될 수 있다. 한편, 두번째 방법에 따라, 부정 변경이 어려운 소프트웨어가 사용되고, 실행 콘텐츠가 ICE(디버거(debugger))에 의해 디코딩되더라도 작업 실행 순서는 의미없을 수 있거나(이 경우, 이전 및 이후의 작업에 영향을 주지 않기 위해 작업들이 구분되어서 단일 작업이 의의가 있다), 또는 작업 그 자체가 암호화될 수 있다. 즉, 보안을 향상하기 위한 작업 스케줄러(미니OS; MiniOS)로서 기능들이 구현된다. 제공된 작업 스케줄러는 타겟 프로그램내에 들어있다.

도 22에 도시된 A/V 압축/압축 해제 SAM(163)에 대한 상세한 설명은 하기에 주어진다.

A/V 압축/압축 해제 SAM(163)은 도 22에 도시된 바와 같이 상호 인증 유닛(220), 디코더들(221 및 222), 압축 해제 유닛(223), 및 디지털-워터마크(watermark) 정보 프로세서(224), 및 부분 개시된 프로세서(225)를 포함한다.

상호 인증 유닛(220)은 A/V 압축/압축 해제 SAM(163)이 SAM(105_{1})으로부터 데이터를 수신하고 세션 키 데이터 K_{ses} 를 생성할 때, 도 30에 도시된 SAM(105_{1})의 상호 인증 유닛(170)을 사용하여 상호 인증을 행한다.

디코더(221)는 세션 키 데이터 K_{ses} 를 이용하여, SAM(105_{1})으로부터 수신된 콘텐츠 키 데이터 K_c , 부분 개시된 파라미터(199), 사용자 디지털 워터마크 정보 데이터(196), 및 콘텐츠 데이터 C를 디코딩한다. 그 후, 디코더(221)는 디코딩된 콘텐츠 키 데이터 K_c 와 콘텐츠 데이터 C를 디코더(222)에 출력하고, 디코딩된 사용자 디지털 워터마크 정보 데이터(196)를 디지털-워터마크 정보 프로세서(224)에 출력하고, 또한 부분 개시된 파라미터(199)를 부분 개시된 프로세서(225)에 출력한다.

디코더(222)는 부분 개시된 프로세서(225)의 제어 하에, 콘텐츠 키 데이터 K_c 를 사용함으로써 부분 개시된 상태에서 콘텐츠 데이터 C를 디코딩하고, 디코딩된 콘텐츠 데이터 C를 압축 해제 유닛(223)으로 출력한다. 디코더(222)는 또한, 정규 동작 모드, 즉 부분 개시된 모드 이외의 다른 모드에서 콘텐츠 키 데이터 K_c 를 사용하여 전체 콘텐츠 데이터 C를 디코딩한다.

압축 해제 유닛(223)은 디코딩된 콘텐츠 데이터 C를 압축 해제하고, 압축 해제된 것을 디지털-워터마크 정보 프로세서(224)로 출력한다. 압축 해제 유닛(223)은 예를 들어 ATRAC3 방법에 따라 예를 들어, 도 3a에 도시된 콘텐츠 파일 CF에 저장된 A/V 압축 해제 소프트웨어를 사용함으로써, 콘텐츠 데이터 C를 압축 해제한다.

디지털-워터마크 정보 프로세서(224)는 디코딩된 사용자 디지털 워터마크 정보 데이터(196)에 따라 사용자 디지털 워터마크 정보를 디코딩된 콘텐츠 데이터 C에 넣어서, 새로운 콘텐츠 데이터 C를 생성한다. 디지털-워터마크 정보 프로세서(224)는 그 후, 새롭게 생성된 콘텐츠 데이터 C를 재생 모듈(169)로 출력한다.

이러한 방식으로, 사용자 디지털 워터마크 정보는 콘텐츠 데이터 C를 재생할 때, A/V 압축/압축 해제 SAM(163)에 의해 콘텐츠 데이터 C로 넣어진다.

본 발명에서, 사용자 디지털 워터마크 정보 데이터(196)가 콘텐츠 데이터 C에 넣어지지 않은 것이 결정될 수 있다.

부분 개시된 프로세서 (225)는 부분 개시된 파라미터 (199)에 기초되어 디코더 (222)에게 통지하고, 블록들은 디코딩 되고, 블록들은 디코딩되지 않는다. 부분 개시된 프로세서 (225)는 예를 들어, 증거 (demonstration)용 재생 기능들을 제한하거나, 증거용 콘텐츠를 청취하기 위한 기간을 제한함으로써, 부분 개시된 모드를 제어할 수 있다.

재생 모듈 (169)은 디코딩되고 압축 해제된 콘텐츠 데이터 C에 따라 재생 동작을 행한다.

SAM (105₁내지 105₄)을 EMD 서비스 센터 (102)에 등록 (register)하기 위한 처리는 이들이 ship될 때 (shipped), 다음과 같이 이루어진다. 동일한 등록 처리가 SAM (105₁내지 105₄)에서 행해지므로 SAM (105₁)의 등록만이 하기에서 논의 된다.

SAM (105₁)을 ship할 때, 다음 키 데이터가 EMD 서비스 센터 (102)의 키 서버 (141)에 의해 SAM 관리자 (149)를 통해, 도 30에 도시된 저장 유닛 (192)에 등록된다.

SAM (105₁)이 ship될 때, 예를 들어 SAM (105₁)에 의해 EMD 서비스 센터 (102)로의 초기 액세싱을 위해 사용된 프로그램 또한, 저장 유닛 (192)에 저장된다.

보다 구체적으로는, SAM (105₁)은 초기 등록으로, 예를 들어 SAM (105₁)의 식별자 SAM_ID, 저장 키 데이터 $K_{SR,K}$, 근원 확인 기관 (92)의 공개 키 데이터 $K_{R,CA}$, EMD 서비스 센터 (102)의 공개 키 데이터 $K_{ESC,R}$ SAM (105₁)의 전용 키 데이터 $K_{SAM,I,S}$, 공개 키 증명 데이터 CER_{SAM} , 서명 데이터 $SIG_{Z,ESC}$, 및 A/V 압축/압축 해제 SAM (163)과 매체 SAM과의 사이에서 인증 키 데이터를 생성하는 소스 키 데이터를 저장하고, 모든 데이터들은 도 34에 도시된 바와 같이, 데이터의 원편에 첨부된 심볼 " ★ "를 갖는다.

공개 키 증명 데이터 CER_{SAM} 은 SAM (105₁)이 ship된 후 등록될 때, EMD 서비스 센터 (102)로부터 SAM (105₁)으로 전송될 수 있다.

SAM (105₁)을 ship할 시, 도 3a 및 3b에 각각 도시된 콘텐츠 파일 CF와 키 파일 KF의 판독 포맷을 정하는 파일 판독기가 EMD 서비스 센터 (102)에 의해 저장 유닛 (192)으로 기입된다. 그 후, SAM (105₁)에서, 저장 유닛 (192)에 저장된 파일 판독기는 콘텐츠 파일 CF 및 키 파일 KF에 저장된 데이터를 판독할 때, 사용된다.

근원 확인 기관 (92)의 공개 키 데이터 $K_{R,CA}$ 는 리버 - 새머 - 애들먼 (River0Shamir - Adleman; RSA) 알고리즘을 사용하고, 이것은 인터넷상의 전자 상거래에 종종 사용되며, 그 데이터 길이는 예를 들어, 1024 비트이다. 공개 키 데이터 $K_{R,CA}$ 는 도 1에 도시된 근원 확인 기관 (92)에 의해 발행된다.

EMD 서비스 센터 (102)의 공개 키 데이터 $K_{ESC,R}$ 는 타원형 곡선 암호법 (elliptic curve cryptosystem)에 의해 생성되고, 그 암호 길이는 RSA와 비교될 수 있거나 그것보다 더 크며, 데이터 길이는 예를 들어, 160 비트 뿐이다. 그러나, 암호화 강도를 고려할 때, 공개 키 데이터 $K_{ESC,P}$ 는 192 비트 이상인 것이 바람직하다. EMD 서비스 센터 (102)는 근원 확인 기관 (92)에 공개 키 데이터 $K_{ESC,P}$ 를 등록한다.

근원 확인 기관(92)은 공개 키 데이터 $K_{ESC,P}$ 의 공개 키 증명서 데이터 CER_{ESC} 를 생성한다. 공개 키 데이터 $K_{ESC,P}$ 를 저장하는 공개 키 증명서 데이터 CER_{ESC} 는 SAM(105₁)에 탑재될 때 저장부(192)에 바람직하게 저장되는 것이 바람직하다. 이 경우, 공개 키 증명서 데이터 CER_{ESC} 는 근원 확인 기관(92)의 전용 키 데이터 $K_{ROOT,S}$ 로 서명된다.

EMD 서비스 센터(102)는 난수를 발생시켜, SAM(105₁)의 전용 키 데이터 $K_{ROOT,S}$ 를 생성하고, 공개 키 데이터 $K_{ESC,P}$ 를 생성하여 전용 키 데이터 $K_{ROOT,S}$ 와 쌍을 이루게 한다.

EMD 서비스 센터(102)는 근원 확인 기관(92)으로부터 증명서를 획득하여 공개 키 데이터 $K_{ESC,P}$ 의 공개 키 증명서 데이터 CER_{ESC} 를 발행하고, 서명 데이터를 EMD 서비스 센터(102)의 전용 키 데이터 $K_{ROOT,S}$ 에 부착한다. 즉, EMD 서비스 센터(102)는 제2 증명 기관의 역할을 한다.

EMD 서비스 센터(102)의 제어하에, 고유 식별자 SAM_ID가 EMD 서비스 센터(102)로부터 SAM(105₁)에 할당된다. 고유 식별자 SAM_ID는 저장부(192) 내에 저장되고, EMD 서비스 센터(102)에 의해 관리된다.

탑재된 후, SAM(105₁)은 사용자 등에 의해 EMD 서비스 센터(102)에 접속되고 등록된다. 그 다음, 라이선스 키 데이터(KD₁ 내지 KD₃)가 EMD 서비스 센터(102)에서 저장부(192)로 전송된다.

즉, SAM(105₁)의 사용자는 콘텐츠를 다운로드받기 전에 EMD 서비스 센터(102)에 등록해야 한다. 이러한 등록은, SAM(105₁)이 로드되는 기기(본 예에서는 네트작업 장치(1601)에 부착된 등록 용지에 사용자를 특정하기 위한 정보(사용자 성명, 주소, 연락 전화번호, 성, 예금 계좌, 로그인 네임, 패스워드 등)를 기입함으로써, 우편 등에 의해 오프라인으로 수행된다. 전술한 등록이 수행될 때까지, 사용자는 SAM(105₁)을 이용할 수 없다.

EMD 서비스 센터(102)는 사용자의 등록에 따라 사용자마다 고유한 식별자를 발생하며, 계좌를 처리하는 데에 이용되는 SAM_ID와 USER_ID 간의 관계를 관리한다.

EMD 서비스 센터(102)는 SAM(105₁) 사용자의 초기 이용을 위한 정보 참조 식별자 ID와 패스워드를 할당하고, 이것을 사용자에게 보고한다. 사용자는 정보 참조 식별자 ID 및 패스워드를 이용하여 콘텐츠 데이터의 현재 사용 상태 등에 관한 질문을 EMD 서비스 센터(102)에 발행한다.

EMD 서비스 센터(102)는 신용 카드 회사에 문의하여 사용자의 신분을 체크하거나 사용자 등록시에 사용자에게 오프라인으로 사용자 자신의 신분을 문의할 수 있다.

이제, 도 34에 도시된 바와 같이 SAM(105₁) 내의 저장부(192)에서의 SAM 등록 리스트를 저장하기 위한 프로세스가 설명된다.

도 1에 도시된 SAM(105₁)은, IEEE-1394 직렬 버스 등에 접속된 기기에 전원이 공급될 때나 새로운 기기가 버스(191)에 접속될 때 생성된 토폴로지 맵을 이용하여, SAM(105₁) 자신과 동일한 시스템인 SAM(105₂ 내지 105₄)의 SAM 등록을 얻는다.

토폴로지 맵은, SAM(105₁ 내지 105₄)는 물론, 도 58에 도시되어 있는 바와 같이 버스(191)에 접속되어 있는 A/V 기기(106₅ 및 106₆)의 SCMS 처리 회로(105₅ 및 105₆)에 대해서도, 버스(191)를 따라 생성된다. 따라서, SAM(105₁)은 토폴로지 맵으로부터 SAM(105₁ 내지 105₄)에 관한 정보를 추출함으로써, 도 59에 도시된 SAM 등록 리스트를 생성한다.

그 다음, SAM(105₁)은 도 59에 도시된 SAM 등록 리스트를 EMD 서비스 센터(102)에 등록하여 서명을 얻는다.

전술한 프로세스는 버스(191)의 세션을 이용하여 SAM(105₁)에 의해 자동적으로 실행되며, SAM(105₁)은 EMD 서비스 센터(102)의 SAM 등록 리스트의 등록 커맨드를 발행한다.

SAM(105₁)으로부터 도 59에 도시된 SAM 등록 리스트를 수신하면, EMD 서비스 센터(102)는 유효 기간을 체크하고, 등록동안 SAM(105₁)에 의해 지정되는 조정 기능도 체크한다. EMD 서비스 센터(102)는 도 60에 도시되어 있는 것과 같은 미리 저장된 취소 리스트(증명서 취소 리스트(CRL))를 참조하고, SAM 등록 리스트 내에 취소 플래그를 설정한다. 취소 리스트는 불법적인 사용으로 인해 사용이 금지된(무효화된) SAM의 리스트이다. SAM들 간의 통신을 수행하는 데 있어서, 각각의 SAM은 해당 SAM이 무효화되어 그들 간의 통신이 단절되었는지의 여부를 알기 위해 취소 리스트를 체크한다.

계좌를 처리하는 데 있어서, EMD 서비스 센터(102)는 리스트 내에 기술된 SAM이 취소 리스트 내에 포함되어 있는지의 여부를 알기 위해 SAM(105₁)의 SAM 등록 리스트를 체크한다. 또한, EMD 서비스 센터(102)는 SAM 등록 리스트에 서명을 부착한다.

그 결과, 도 61에 도시된 SAM 등록 리스트가 생성된다.

SAM 취소 리스트는 동일 시스템 내의 SAM들에 대해 형성되며 (즉, 버스(101)에 접속된 SAM들), 각각의 SAM이 해당 SAM의 취소 플래그에 따라 무효화되었는지의 여부를 나타낸다.

취소 리스트 CRL는, EMD 서비스 센터(102)로부터 SAM으로 전송된 업데이트 데이터에 따라 SAM 내에서 자동적으로 업데이트되는 것이 바람직하다. SAM의 보안 기능은 다음과 같다.

보안 기능으로서, SAM은 공통 키 암호법의 DES(3중 DES/강화된 암호 표준(AES)), 공통 키 암호법의 타원 곡선 암호법(서명 생성/EC-DSA 체크, 공통 키 생성 EC-DH, 및 공통 키 암호법 EC-ElGamal), 압축 기능(해쉬 함수) SH A-1, 및 난수 생성기(고유 난수)와 같은 암호 라이브러리의 IP 성분을 처리한다.

공개 키 암호법(타원 곡선 암호법)은 상호 인증, 서명 생성, 서명 체크, 및 공통 키(세션키) 생성(전달)에 채용된다. 공통 키 암호법(DES)은 콘텐츠의 암호화 및 암호해제화에 채용되며, 압축 기능(해쉬 함수)은 신호 생성 및 체크시의 메시지 인증에 채용된다.

도 62는 SAM의 보안 기능을 도시하고 있다. SAM에 의해 관리되는 보안 기능은, (1) 콘텐츠를 암호화하고 암호해제하기 위한 애플리케이션층에서의 보안 기능과 (2) 다른 SAM과의 상호 인증을 수행함으로써 공통 키를 보안하기 위한 물리층에서의 보안 기능의 2가지 유형이 있다.

EMD 시스템(100)에서, 배포된 콘텐츠 데이터 C는 완전히 암호화되며, 키는 계좌 처리에 의해 구입된다. USP 데이터(106)는 인-밴드 시스템에 따라 콘텐츠 데이터 C와 함께 전송되기 때문에, 네트작업 매체의 종류와 무관하게, 한 층에서 관리된다. 따라서, 위성, 지상파, 케이블, 무선 또는 기록 매체 등과 같은 통신 경로의 종류와 무관하게, 공통 권리 처리 시스템을 제공하는 것이 가능하다. 예를 들어, UCP 데이터(106)가 네트작업의 물리층의 프로토콜의 헤더에 삽입되면, 동일한 종류의 UCP 데이터(106)에 대해서도, 각각의 네트작업이 USP 데이터(106)의 삽입 장소를 결정할 필요가 있다.

본 실시예에서, 콘텐츠 데이터 C 및 키 파일 KF는 보호를 위해 애플리케이션층에 의해 암호화된다. 상호 인증은 물리층, 전송포스트층 또는 애플리케이션층에서 수행될 수 있다. 암호화 기능을 물리층에 일체화시킨다는 것은, 암호화 기능을 하드웨어에 일체화시킨다는 의미이다. 상호 인증을 수행하는 주된 목적은 발신자와 수신자 간의 통신 경로를 보장하는 것이므로, 상호 인증은 물리층에서 수행되는 것이 바람직하다. 그러나, 실제에 있어서, 상호 인증은 전송 채널과 무관하게 전송포스트층에서 구현되는 경우가 많다.

SAM의 보안 기능은, 통신하고자 하는 다른 SAM의 보전을 검토하기 위한 상호 인증과, 애플리케이션층에서의 계좌 처리를 포함하는 콘텐츠 데이터의 암호화 및 암호해제화를 포함한다.

일반적으로, 기기들 간에서 통신을 수행하기 위한 SAM들 간의 상호 인증은 애플리케이션층에서 구현된다. 그러나, 트랜스포트층이나 물리층과 같은 다른 층에서도 구현될 수 있다.

물리층에서 구현되는 상호 인증은 5C1394CP(콘텐츠 보호)를 이용한다. 1394CP에 따르면, 공통 키 암호법인 M6는 1394LINKIC(하드웨어)의 등시성 채널에서 구현된다. 그러면, 상호 인증(타원 곡선 암호법 또는 해시 함수를 이용한 공통 키 암호법)은 비등시성 채널을 이용하여 수행되며, 그 결과적인 세션키는 등시성 채널의 M6에 전송된다. 따라서, 공통 키 암호법은 M6에 의해 구현된다.

SAM들 간의 상호 인증이 물리층의 하드웨어에서 구현되는 경우, 공개 키 암호법(타원 곡선 암호법)을 이용하여 상호 인증을 수행함으로써 얻어지는 세션키는 호스트 CPU를 통해 1394LINKIC의 M6에 전송되며, 따라서 1394CP에 의해 얻어진 세션키와 함께 상기의 세션키를 이용하여 콘텐츠 데이터가 암호화된다.

SAM들 간의 상호 인증이 애플리케이션층에서 수행되는 경우, 콘텐츠 데이터 C는 SAM 내에서 공통 키 암호법 라이브러리(DES/3중 DES/AES)를 이용하여 암호화된다.

본 실시예에서, 예를 들어, SAM들 간의 상호 인증은 애플리케이션 층에서 구현되며, 1394CP에 의한 상호 인증은 1394LINKIC와 같은 물리층에서 구현된다.

이 경우, 계좌 처리를 포함하는 콘텐츠 데이터 C의 암호화 및 암호해제화는 애플리케이션층에서 수행된다. 그러나, 애플리케이션층은 사용자가 액세스하기 쉽고 무제한적으로 분석될 수 있다. 따라서, 본 실시예에서, 계좌 관련 처리는, 처리 콘텐츠를 외부 소스로부터 전혀 모니터링할 수 없어서 부정 변경이 매우 어려운 하드웨어 내에서 실행된다. 이것이 SAM을 부정 변경이 어려운 하드웨어로 구현하는 주된 이유이다.

계좌 처리가 호스트 CPU 내에서 실행되는 경우, 부정 변경이 어려운 소프트웨어는 CPU 내에서 구현된다.

이제, 도 63을 참조하여, 예를 들어 도 1에 도시된 사용자 홈 네트작업(103)의 네트작업 장치(160₁) 내의 다양한 SAM의 구현예가 설명된다.

도 63에 도시되어 있는 바와 같이, 네트작업 장치(160₁)는 호스트 CPU(810₁), SAM(105₁), 다운로드 메모리(167), 매체 드라이브 SAM(260), 및 다이내믹 RAM(DRAM)(1004)과 같은 드라이브 CPU(1003) 및 충격 방지(멜팅 방지) 메모리를 포함한다.

다운로드 메모리의 부분과 충격 방지 메모리(1004)의 부분은 공통 메모리로서 이용되며, 이것은 SAM(105₁)과 호스트 CPU(810₁)로부터 액세스될 수 있다.

충격 방지 메모리(1004)는 데이터 버스(1002)를 통해 수신된 콘텐츠 데이터 C를 저장한 후, A/V 압축/압출 해제 SAM(163)으로 출력한다. 이것은, 기록 매체(130)로부터의 콘텐츠 데이터 C의 판독 동작이 진동 등에 의해 중단되는 경우에도, 콘텐츠 데이터 C가 A/V 압축/압출 해제 SAM(163)에 계속적으로 출력될 수 있게 한다. 따라서, 콘텐츠 데이터 C의 재생 동작이 중단되는 것을 효과적으로 방지할 수 있다.

다운로드 메모리(167)는 메모리 제어기 및 버스 아비터/브리지들을 포함하는 모듈(1005)을 통해 호스트 CPU 버스(1000)에 접속된다.

도 64는 모듈(1005) 및 주변 회로의 상세한 구성을 도시하고 있다. 도 64에 도시한 바와 같이, 모듈(1005) 및 버스 아비터 브리지(1501)를 포함한다.

제어기(1500)는 DRAM이 다운로드 메모리(167)로 사용되는 때에 DRAM 인터페이스(I/F)의 기능을 하며, 판독/기입(r/w)선, 어드레스 버스, CAS선 및 RAS선을 포함하여 다운로드 메모리(167)와 통신한다.

버스 아비터/브리지(1501)는 호스트 CPU 버스(1000)와의 중재를 수행하며, 다운로드 메모리(167)와 통신하기 위한 데이터 버스를 갖고, r/w선, 어드레스 버스, 데이터 버스 및 대기선을 포함하여 SAM(105₁)과 통신한다. 버스 아비터/브리지(1501)는 호스트 CPU 버스(1000)에 접속된다.

버스 아비터/브리지(1501), 호스트 CPU(810₁) 및 SAM(105₁)은 호스트 CPU 버스(1000)에 접속된다. 호스트 CPU 버스(1000)는 CS선, r/w선, 어드레스 버스, 데이터 버스 및 대기선을 갖는다.

다운로드 메모리(167) 및 충격 방지 메모리(1004)는 상술한 콘텐츠 파일 CF 및 키 파일 KF를 저장한다. 공통 메모리로서 이용되는 저장 영역 이외의 충격 방지 메모리(1004)의 저장 영역은, 콘텐츠 데이터 C가 A/V 압축/압축 해제 SAM(163)으로 출력될 때까지 매체 드라이브 SAM(260)으로부터 수신된 콘텐츠 데이터 C를 임시로 저장하는 데에 이용된다.

A/V 압축/압축해제 SAM(163)은 데이터를 호스트 CPU 버스(1000)를 통하여 다운로드 메모리(167)로 전송하고, 또한 데이터를 데이터 버스(1002)를 통하여 매체 드라이브 SAM(260)으로 전송한다.

다운로드 메모리(167) 뿐만 아니라, SAM(105₁), A/V 압축/압축해제 SAM(163), 및 DMA(1010)는 호스트 CPU 버스(1000)에 접속되어 있다.

DMA(1010)는 호스트 CPU(810₁)로부터의 커맨드에 따라 중앙 집중적으로 호스트 CPU 버스(1000)를 통하여 다운로드 메모리(167)에 대한 액세스를 제어한다.

호스트 CPU 버스(1000)는 또한 다른 SAM들, 즉, SAM들(105₂ 내지 105₄)와의 통신을 위하여, 사용자 가정 네트워크(103) 내에서 1394-직렬 인터페이스 링크계층을 이용하여 채택된다.

드라이브 CPU(1003), 매체 드라이브 SAM(260), RF 증폭기(1006), 매체 SAM 인터페이스(1007), 및 DMA(1011)는 드라이브 CPU 버스(1001)에 접속된다.

드라이브 CPU(1003)는 디스크형 레코딩 매체(130)에 대한 액세스를 호스트 CPU(810₁)로부터의 커맨드에 따라 중앙 집중적으로 제어한다. 이 경우에, 호스트 CPU(810₁)는 마스터의 역할을 하는 한편, 드라이브 CPU(1003)은 슬레이브의 역할을 한다. 드라이브 CPU(1003)는 호스트 CPU(810₁)의 관점에서 I/O 로써 취급된다.

드라이브 CPU(1003)는 레코딩 매체(RAM)(130)를 액세스하면서 데이터를 인코딩/디코딩 한다.

레코딩 매체(RAM)(130)이 드라이브에서 설정될 때, 드라이브 CPU(1003)는 레코딩 매체(130)가 SAM(105₁)(EMD 시스템(100))에 적합한지를 (즉, 권리 처리가 SAM(105₁)에 의하여 레코딩 매체(130) 상에서 안전하게 수행될 수 있는지를) 판정한다. 만약 그렇다면, 드라이브 CPU(1003)는 대응하는 정보를 호스트 CPU(810₁)로 리포트하고, 또 매체 드라이브 SAM(260)에게 매체 SAM(133)과 함께 상호 인증을 수행하라고 명령한다.

매체 SAM 인터페이스(1007)는 드라이브 CPU 버스(1001)를 통하여 레코딩 매체(130)의 매체 SAM(133)에 대한 액세스를 위하여 인터페이스의 역할을 한다.

DMA(1011)는 드라이브 CPU 버스(1001) 및, 드라이브 CPU(1003)로부터의 커맨드에 따른 데이터 버스(1002)를 통하여 쇼크 증명 메모리(1004)에 대한 액세스를 중앙 집중적으로 제어한다. DMA(1011)는 예를 들어, 매체 드라이브 SAM(260)과 쇼크 증명 메모리(1004) 사이의 데이터 전송을 데이터 버스(1002)를 통하여 제어한다.

예를 들어, 도 63에 도시된 구성에 따라, SAM(105₁)과, 레코딩 매체(130)의 매체 SAM(133) 사이의 상호 인증과 같은 통신을 수행하는 데 있어서, 데이터 전송이 그 사이에서 호스트 CPU 버스(1000), 호스트 CPU(810₁), 드라이브 CPU(1003) 내의 레지스터, 드라이브 CPU 버스(1001), 및 호스트 CPU(810₁)의 제어에 기초한 매체 SAM 인터페이스(1007)를 통하여 행해진다.

레코딩 매체(130)를 액세스하는데 있어서, 상호 인증은 매체 드라이브 SAM(260)과 매체 SAM(133)의 사이에서 행해진다.

다운로드 메모리(167) 또는 쇼크 증명 메모리(1004)를 액세스하기 위하여 A/V 압축/압축해제 SAM(163)에서 데이터를 압축 또는 압축해제하는데 있어서, 상술한 바와 같이, 상호 인증은 SAM(105₁)과 A/V 압축/압축해제 SAM(163) 사이에서 수행된다.

이 실시예에 있어서, 도 63에서는 SAM(105₁)과 A/V 압축/압축해제 SAM(163)는 호스트 CPU(810₁)로부터의 관점에서 I/O 인터페이스에 접속된 장치로서 취급된다. SAM(105₁)과 호스트 CPU(810₁)를 갖는 A/V 압축/압축해제 SAM(163)의 통신 및 데이터 전송은 메모리 I/O와 어드레스 디코더(1020)의 제어 하에 수행된다. 이 경우에, 호스트 CPU는 마스터(810₁)의 역할을 하는 한편, A/V 압축/압축해제 SAM(163)은 슬레이브의 역할을 한다. SAM(105₁)과 A/V 압축/압축해제 SAM(163)은 호스트 CPU(810₁)에 의해 명령된 처리를 실행하고, 필요하다면 그 결과를 호스트 CPU(810₁)로 리포트한다.

매체 SAM(133)과 매체 드라이브 SAM(260)은 드라이브 CPU(1003)로부터의 관점으로써 I/O 인터페이스에 접속된 장치로서 취급된다. 매체 SAM(133)과 드라이브 CPU(1003)를 갖는 매체 드라이브 SAM(260)의 통신과 데이터 전송은 메모리 I/O와 어드레스 디코더(1021)의 제어 하에 수행된다. 이 경우에, 드라이브 CPU(1003)는 마스터의 역할을 하는 한편, 매체 SAM(133)과 매체 드라이브 SAM(260)은 슬레이브의 역할을 한다. 매체 SAM(133)과 매체 드라이브 SAM(260)은 드라이브 CPU(1003)에 의해 명령된 처리를 실행하고, 필요하다면, 그 결과를 드라이브 CPU(1003)로 리포트한다.

다운로드 메모리(167)와 쇼크 증명 메모리(1004)에 저장된 콘텐츠 파일 CF와 키 파일 KF에 대한 액세스 제어는 SAM(105₁)에 의해 중앙 집중적으로 수행될 수 있다. 다른 방안으로, 콘텐츠 파일 CF에 대한 액세스 제어는 호스트 CPU(810₁)에 의해 수행될 수 있고, 키 파일 KF에 대한 액세스 제어는 SAM(105₁)에 의해 수행될 수 있다.

드라이브 CPU(1003)에 의해 레코딩 매체(130)로부터 판독된 콘텐츠 데이터 C는 RF 증폭기(1006)와 매체 드라이브 SAM(260)를 통하여 쇼크 증명 메모리(1004)에 저장되고, 그후 A/V 압축/압축해제 SAM(163)에 의해 압축해제된다. 압축해제된 콘텐츠 데이터는 디지털-아날로그(D/A) 변환기에서 아날로그 데이터로 변환되고, 변환된 아날로그 신호에 기초한 음향은 스피커로부터 출력된다.

이 경우에, 쇼크 증명 메모리(1004)는 복수개의 트랙으로 이루어진 콘텐츠 데이터 C를 일시적으로 저장할 수 있으며, 이것은 레코딩 매체(130)에 불연속적으로 놓여 있는 저장 영역으로부터 비연속적으로 판독되고, 그 후 콘텐츠 데이터 C를 A/V 압축/압축해제 SAM(163)으로 연속적으로 출력한다.

도 63에 도시된 사용자 가정 네트워크(103) 내의 다양한 SAM들의 마스터-슬레이브 관계성은 아래에 설명된다.

예를 들어, 구매 모드가 결정되는 콘텐츠 데이터 C가 도 65에 도시된 것처럼, 레코딩 매체(130) 상에 레코딩될 때, 호스트 CPU(810₁)는 내부 인터럽트를 출력하여, I/O 장치의 역할을 하는 SAM(105₁)에게 콘텐츠 데이터 C의 구매 모드를 판정하고, 또 레코딩 매체(130)의 매체 SAM(133)과의 상호 인증을 수행하고 명명하여, 콘텐츠 데이터 C를 레코딩 매체(130) 상에 레코딩한다.

이 경우에, 호스트 CPU(810₁)는 마스터로서 역할을 하는 한편, SAM(105₁)과 레코딩 매체(130)는 슬레이브로서 역할을 한다. 레코딩 매체(130)는 호스트 CPU(810₁)로부터의 관점에서 I/O 장치로서 취급된다.

호스트 CPU(810₁)로부터의 내부 인터럽트에 응답하여, SAM(105₁)은 매체 SAM(133)과 통신하여 콘텐츠 데이터 C의 구매 모드를 결정하고, 또한 콘텐츠 키 데이터 KC와 같은 미리 결정된 키 데이터를 매체 SAM(133)에 기록한다. 이 처리를 완료하고 나서, SAM(105₁)은 처리 결과를 외부 인터럽트를 통하여 혹은 호스트 CPU(810₁)를 폴링하는 것에 의하여 호스트 CPU(810₁)로 리포트한다.

구매 모드를 결정하기 위한, 레코딩 매체 상에 레코딩된 콘텐츠 데이터 C를 재생하는데 있어서, 콘텐츠 데이터 C를 재생하라는 명령이 도 66에 도시된 것처럼 내부 인터럽트를 통하여 호스트 CPU(810₁)로부터 SAM(105₁)로 주어진다.

내부 인터럽트에 응답하여, SAM(105₁)은 키 파일 KF과 같은 키 데이터 블록을 레코딩 매체(130)의 매체 SAM(133)으로부터 판독하고, 키 데이터 블록에 저장된 UCS 데이터(166)에 기초한 콘텐츠 데이터 C를 재생하기 위한 처리를 실행한다.

SAM(105₁)은 내부 인터럽트를 출력하여 A/V 압축/압축해제 SAM(163)에게 레코딩 매체(130)로부터 판독된 콘텐츠 데이터 C를 압축해제하라고 명령한다.

SAM(105₁)로부터 내부 인터럽트를 수신하면, A/V 압축/압축해제 SAM(163)은 레코딩 매체(130)로부터 판독된 콘텐츠 데이터 C를 디스크램블하고, 디지털 워터마크 정보를 맵핑하고 검출하며, 콘텐츠 데이터를 압축해제한다. 그후, A/V 압축/압축해제 SAM(163)은 콘텐츠 데이터 C를 재생하도록 하기 위하여, 처리된 콘텐츠 데이터 C를 D/A 변환기로 출력한다.

재생 동작의 완료 후에, A/V 압축/압축해제 SAM(163)은 대응하는 정보를 SAM(105₁)으로 리포트한다.

상술한 정보를 수신하면, SAM(105₁)은 그것을 외부 인터럽트를 통하여 호스트 CPU(810₁)로 리포트한다.

이 경우에, 호스트 CPU(810₁)과 SAM(105₁) 사이의 관계성에 있어서, 호스트 CPU(810₁)은 마스터의 역할을 하는 한편, SAM(105₁)은 슬레이브의 역할을 한다. SAM(105₁)과 A/V 압축/압축해제 SAM(163) 사이의 관계성에 있어서, SAM(105₁)은 마스터의 역할을 하는 한편, A/V 압축/압축해제 SAM(163)은 슬레이브의 역할을 한다.

비록 이 실시예에서 A/V 압축/압축해제 SAM(163)이 SAM(105₁)을 위한 슬레이브 일지라도, 그것은 호스트 CPU(810₁)를 위한 슬레이브일 수도 있다.

만약 레코딩 매체(130) 상에 레코딩된 콘텐츠 데이터가, 도 67에 도시된 것처럼, 콘텐츠 데이터의 권리 처리를 수행하지 않고 재생된다면, 호스트 CPU(810₁)는 내부 인터럽트를 출력하여 A/V 압축/압축해제 SAM(163)에게 레코딩 매체(130)로부터 콘텐츠 데이터를 판독하라고 명령한다.

내부 인터럽트를 수신하면, 매체 드라이브 SAM(260)은 디코더에서 레코딩 매체(130)로부터 판독된 콘텐츠 데이터를 디코드하고, 그 후 그것을 쇼크 중명 메모리(1004)에 저장한다. 이 처리를 완료하면, 매체 드라이브 SAM(260)은 대응하는 정보를 외부 인터럽트를 통하여 호스트 CPU(810₁)로 리포트한다.

쇼크 중명 메모리(1004)에 저장된 콘텐츠 데이터는 A/V 압축/압축해제 SAM(163)으로 판독되고, 디지털 워터마크 정보를 디스크램블링, 맵핑, 및 검출하는 것과 같은 처리를 겪고, 그후 D/A 변환기를 통하여 재생된다.

이 처리의 완료 후에, A/V 압축/압축해제 SAM(163)은 이 정보를 호스트 CPU(810₁)로 외부 인터럽트를 통하여 리포트한다.

이 경우에, 호스트 CPU(810₁)는 마스터의 역할을 하는 한편, A/V 압축/압축해제 SAM(163)과 매체 드라이브 SAM(260)은 슬레이브의 역할을 한다.

사용자 가정 네트작업(103) 내에서 SAM의 상술한 기능을 수행하기 위한 회로 모듈들은 아래에 설명된다.

상기에서 논의된 것처럼, 사용자 가정 네트작업(103) 내에서 SAM은 구매 모드를 결정하는 것과 같은 권리 처리(이의 배분)를 수행하기 위한 SAM들(105)(105₁ 내지 105₄), 레코딩 매체에 배치된 매체 SAM(133), A/V 압축/압축해제 SAM(163), 및 매체 드라이브 SAM(260)을 포함한다. 상술한 SAM을 위하여 제공된 회로 모듈들은 다음과 같다.

권리 처리 SAM의 예시

도 68은 권리 처리 SAM(105a)을 위한 회로 모듈을 도시한다.

SAM(105a)은 조작 방지 하드웨어(본 발명의 회로 모듈과 동등함)이며, 도 68에 도시된 바와 같이, CPU(1100), DAM(1101), MMU(1102), I/O 모듈(1103), 마스크 ROM(1104), 불휘발성 메모리(1105), 작업 RAM(1106), 공개 키 암호화 모듈(1107), 공통 키 암호화 모듈(1108), 해쉬 기능 모듈(1109), (고유의) 무작위 번호 발생기(1110), 실시간 클럭 모듈(1111), 및 외부 버스 I/F(1112)를 포함한다.

관리 처리 SAM(105a)의 소자들과 본 발명의 소자들의 관계성은 다음과 같다. CPU(1100)은 산술 처리 회로에 대응한다. 마스크 ROM(1104), 불휘발성 메모리(1105), 및 작업 RAM(1106)은 저장 회로에 대응한다. 공개 키 암호화 모듈(1108)은 암호화 처리 회로에 대응한다. 외부 버스 I/F(1112)는 외부 버스 인터페이스에 대응한다.

도 69를 참조로 하여 아래에 설명되는 것처럼, 내부 버스(1120과 1121)는 본 발명의 제1 버스에 대응하고, 외부 버스(1123)는 본 발명의 제2 버스에 대응한다.

내부 버스(1120)는 또한 제3 버스에 대응하고 내부 버스(1121)는 또한 제4 버스에 대응한다.

외부 버스 I/F(1112)는 제1 인터페이스 회로에 대응하고, 버스 I/F 회로(1116)는 제2 인터페이스 회로에 대응한다.

내부 버스(1122)는 제5 버스에 대응하고, I/O 모듈은 제3 인터페이스 회로에 대응하고, 버스 I/F 회로(1117)는 제4 인터페이스 회로에 대응한다.

도 30에 도시된 SAM(105₁)의 기능 모듈과 도 68에 도시된 회로 모듈 사이의 관계성에 관한 간략한 설명은 아래에 제공된다.

CPU(1100)는 예를 들어, 마스크 ROM(1104)과 불휘발성 메모리(1105)에 저장된 프로그램을 실행하여, 도 30에 도시된 CPU(1100), 회계 처리기(187), 및 이용 모니터(186)의 기능들을 수행한다.

DMA(1101)는 도 22에 도시된 다운로드 메모리(167)와 도 30에 도시된 저장 유닛(192)에 대한 액세스를 CPU(1100)로부터의 커맨드에 응답하여 중앙 집중적으로 제어한다.

MMU(1102)는 도 22에 도시된 다운로드 메모리(167)의 어드레스 공간과 도 30에 도시된 저장 유닛을 관리한다.

I/O 모듈(1103)은 도 30에 도시된 매체 SAM 매니저(197)의 기능들의 일부를 수행한다.

마스크 ROM(1104)은, SAM(105₁)을 제조할 때, SAM(105₁)을 위한 초기와 프로그램 및 무결성 체크 프로그램과 같은, 고정된 프로그램과 데이터를 저장하고, 도 30에 도시된 저장 유닛(192)의 기능들의 일부를 수행한다.

불휘발성 메모리(1105)는 암호화 프로그램 및 키 데이터와 같은, 다양한 프로그램과 데이터를 저장하고, 도 30에 도시된 저장 유닛(192)의 기능들의 일부를 수행한다.

작업 RAM(1106)은 도 30에 도시된 작업 메모리(200)에 대응한다.

공개 키 암호 모듈(1107)은 도 30에 도시된 신호 처리기(189)의 기능의 일부를 실행하며, 공개 키 암호 해독법에 따라 매체 SAM(133)과 상호 인증을 수행하고, SAM(105)의 서명 데이터를 생성하고, (EMD 서비스 센터(102), 서비스 공급자(101)의, 제2 실시예에서는 서비스 공급자(310)의) 서명 데이터를 채킹하고, 전송될 소량의 데이터(키 파일 KF와 같은)의 암호화 및 암호 해독과 및 키의 공유에 사용된다. 공개 키 암호화 모듈(1107)은 회로 모듈(하드웨어(H/W) IP 솔루션)로 실행되거나 CPU(1100)(소프트웨어(S/W) IP 솔루션)에 의해 불휘발성 메모리(1105)에 저장된 공개 키 암호화 프로그램을 실행함으로써 실시될 수도 있다.

공통 키 암호화 모듈(1108)은 서명 처리기(189) 및 암호화/암호 해독화 (디코딩) 유닛(171, 172 및 173)의 기능의 일부를 실행하며, 상호 인증을 수행하고 상호 인증에 의해 얻어진 세션 키 데이터 K_{SES} 를 사용하여 데이터를 암호화하고 암호 해독화하는 데 사용된다. 공통 키 암호 해독법은 공개 키 암호 해독법보다 고속 처리를 실현하므로 예를 들어 대용량의 콘텐츠 데이터(콘텐츠 파일 CF)를 암호화 및 암호 해독하는 데 사용된다. 공통 키 암호화 모듈(1108)은 회로 모듈(H/W IP 솔루션)로서 실행되거나 CPU(1100)(S/W IP 솔루션)에 의해 불휘발성 메모리(1105)에 저장된 공통 키 암호화 프로그램을 실행함으로써 실행될 수도 있다.

상호 인증은 공개 키 암호화 모듈(1107) 및 공통 키 암호화 모듈(1108)중 하나 또는 둘다의 암호화 및 암호 해독화에 의해 수행된다.

공통 키 암호화 모듈(1109)은 도 30에 도시된 서명 처리기(189)의 기능의 일부를 수행하며, 서명 데이터가 생성될 때 데이터의 해시 값(hash value)을 생성하는데 사용된다. 특히, 해시 함수 모듈(1109)은 콘텐츠 공급자(101) 및 EMD 서비스 센터(102)의 서명 데이터를 채점하고 도 44a 내지 44d에 도시된 보안 컨테이너(104x)의 키 파일 KF_1 의 해시값 H_{K1} 을 채점하는 데 사용된다. 해시 함수 모듈(1109)은 회로 모듈(H/W IP 솔루션)로서 실행되거나 CPU(1100)(S/W IP 솔루션)에 의해 불휘발성 메모리(1105)에 저장된 해시 회로 모듈 프로그램을 실행함으로써 실행될 수도 있다.

난수 발생기(1110)는 도 30에 도시된 상호 인증 유닛(170)의 기능의 일부를 실행한다.

실시간 클럭 모듈(1111)은 실시간을 발생하며, 유효 기간이 있는 라이선스 키 데이터 KD를 선택하거나 UCS 데이터(166)로 표시된 유효 기간의 요구 조건이 만족되는지 여부를 결정하는 데 사용된다.

외부 버스 I/F(1112)는 도 30에 도시된 콘텐츠 공급자 관리자(180), 다운로드 메모리 관리자(182) 및 EMD 서비스 센터 관리자(185)의 기능의 일부를 실행한다.

도 69는 SAM(105a) 내의 하드웨어 구성을 도시한다. 도 69에는, 도 68에 도시된 것과 동일한 소자가 동일한 참조 부호로 표시되어 있다.

도 69에 도시된 바와 같이, SAM(105a) 내에는 CPU(1100), 마스크 ROM(1104) 및 불휘발성 메모리(1105)가 SAM/CPU 버스(1120)를 통해 서로 접속된다.

DMA(1101)는 내부 버스(1121)에 접속된다. I²C 인터페이스(1130), 매체 SAM 인터페이스(1131), 메모리 스틱(MS) 인터페이스(1132) 및 IC 카드 인터페이스(1133)는 내부 버스(1122)에 접속된다.

매체 SAM 인터페이스(1131)는 기록 매체(130)의 매체 SAM(133)으로/으로부터 데이터를 전송 및 수신한다. MS 인터페이스(1132)는 메모리 스틱(1140)으로/으로부터 데이터를 전송 및 수신한다. IC 카드 인터페이스(1133)는 IC 카드(1141)로/로부터 데이터를 전송 및 수신한다.

도 63에 도시된, 공개 키 암호화 모듈(1107), 공통 키 암호화 모듈(1108), 해시 함수 모듈(1109), 난수 발생기(1110), 실시간 클럭 모듈(1111), 외부 버스 I/F(1112) 및 외부 메모리(201)는 외부 메모리 I/F(1142)에 접속된다.

SAM/CPU 버스(1120) 및 내부 버스(1121)는 버스 인터페이스(1116)를 통해 접속된다. 내부 버스(1122 및 1121) 및 외부 버스(1123)는 버스 인터페이스(1115)를 통해 접속된다.

상술된 SRAM(1155) 및 SAM 상태 레지스터(1156)는 버스 인터페이스(1115)에 저장된다.

상술된 바와 같이, SRAM 상태 레지스터(1156)는 제1 SAM 상태 레지스터(1156a) 및 제2 SAM 상태 레지스터(1156b)를 갖는다. 호스트 CPU(810₁)에 의해 판독된 SAM(105₁)의 상태를 나타내는 플래그가 제1 SAM 상태 레지스터(1156a)에 설정된다. 업무를 실행하는 요구가 호스트 CPU(810₁)로부터 출력되었는지를 나타내는 플래그가 SAM 상태 레지스터(1156b)에 저장되며, 이러한 플래그는 SAM(105₁)의 CPU로부터 판독된다.

DMA(1101)는 CPU(1100)로부터의 커맨드에 응답하여 내부 버스(1121)를 통해 마스크 ROM(1104), 불휘발성 메모리(1105) 작업 RAM(1106)을 중앙 집중적으로 제어한다.

MMU(1113)는 도 63에 도시된 마스크 ROM(1104), 불휘발성 메모리(1105), 작업 RAM(1106) 및 다운로드 메모리(1167)의 메모리 공간을 관리한다.

어드레스 디코더(1114)는 내부 버스(1121)와 외부 버스(1123) 사이에 데이터가 전송될 때 어드레스 변환을 수행한다.

기록 로크 제어 회로(1135)는 CPU(1100)의 로크 키에 기초하여 플래시 ROM으로 각 데이터 블록을 기록하고 플래시 ROM으로부터 각 데이터 블록을 삭제하는 것을 제어한다.

권리 처리 SAM(105a)의 어드레스 공간에 대해 후술될 것이다.

도 70은 권리 처리 SAM(105a)의 어드레스 공간을 도시한다. 어드레스 공간은 개시 어드레스로부터의 개시, 부트 프로그램, 시스템 구성, 플래시 ROM, 미리 결정된 프로그램, 플래시 ROM용의 디바이스 드라이버, 불휘발성 메모리용 디바이스 드라이버, 도 69에 도시된 작업 RAM(1106), 미리 결정된 프로그램, 도 69에 도시된 SRAM(1106), 외부 메모리(201), Key_TOC/File_System, SAM 등록 리스트, 사용 로그 데이터(108), 도 69에 도시된 공통 키 암호화 모듈(1108용 레지스터, 도 69에 도시된 공개 키 암호화 모듈(1107)용 레지스터, 도 69에 도시된 해쉬 함수 모듈(1109)용 레지스터, 도 69에 도시된 난수 발생기(1110)용 레지스터, 도 69에 도시된 실시간 클럭 모듈(1111)용 레지스터, 현재 시간 레지스터, 유효 기간 레지스터, 제어 레지스터, IC 카드 인터페이스, 매체 SAM 인터페이스, 메모리 스틱 인터페이스 및 I²C 버스 인터페이스를 포함한다.

시스템 구성에 할당된 어드레스 공간의 필드에는, 도 69에 도시된 DAM 및 SMA 상태 레지스터(1156)가 저장된다.

플래시 ROM에 할당된 어드레스 공간의 필드에는, 메인 루틴(커널), 인터럽트 프로그램, 인터럽트 프로그램에 의해 불러지는 서브-루틴, 커맨드 분석기(커맨드와 인터럽트 프로그램의 개시 어드레스간의 관계를 나타내는 표) 및 인터럽트 벡터표가 저장된다.

도 70에 도시된 SAM(105a)의 어드레스 공간에서, SAM 상태 레지스터(1156) 및 SRAM(1155)은 호스트 CPU(810)를 갖는 공통 메모리 공간로서 사용된다.

호스트 CPU(810)의 어드레스 공간은 도 71에 도시된 바와 같이, 개시 어드레스로부터의 개시, 부트 프로그램, 시스템 구성, 코드 ROM, 데이터 ROM, 도 63에 도시된 SAM(105₁)를 공유하는 공통 메모리, 도 63에 도시된 매체 드라이브 SAM(260)을 공유하는 공통 메모리 및 외부 디바이스를 포함한다.

도 69에 도시된 SRAM(1155) 및 SAM 상태 레지스터(1156)는 도 63에 도시된 SAM(105₁)를 공유하는 공통 메모리에 할당된다.

권리 처리 SAM의 다른예

도 72는 권리 처리 SAM(105b)의 회로 모듈을 도시한다. 도 72에서는, 도 69에 도시된 것과 동일한 소자들에는 동일한 참조 번호로 나타내었다.

SAM(105b)은 도 72에 도시된 바와 같이, 보안 메모리(105ba), 호스트 CPU(810), 부정 변경이 어려운(tamper-resistant) 소프트웨어(1130) 및 I/O 모듈(1103)으로 구성된다.

SAM(105b)에서는, 부정 변경이 어려운 소프트웨어(1130)가 도 68에 도시된 CPU(1100)와 동일한 기능을 수행하도록 호스트 CPU(810)에 의해 실행된다. 전술된 바와 같이, 부정 변경이 어려운 소프트웨어(1130)는 외부 소스에서의 처리가 완전히 차폐되어 분석 또는 오버라이드되기 어려운 소프트웨어이다.

보안 메모리(105ba)는 마스크 ROM(1104), 불휘발성 메모리(1105), 작업 RAM(1106), 공개 키 암호화 모듈(1107), 공통 키 암호화 모듈(1108), 해쉬 함수 모듈(1109), (진성) 난수 발생기(1110), 실시간 클럭 모듈(1111) 및 외부 버스 I/F(1112)를 포함하는 부정 변경이 어려운 하드웨어이다.

공개 키 암호화 모듈(1107), 공통 키 암호화 모듈(1108) 및 해쉬 함수 모듈(1109)은 불휘발성 메모리(1105)에 저장되어 있는 공개 키 암호화 프로그램, 공통 키 암호화 프로그램 및 해쉬 함수 프로그램을 호스트 CPU(810) (S/W IP 솔루션)에 의해 각각 실행함으로써 수행될 수도 있다.

상술된 매체 SAM(133)의 구성의 한 예는 다음과 같다. 도 73은 매체 SAM(133)의 회로 모듈을 도시한다.

매체 SAM(133)은 도 73에 도시된 바와 같이, CPU(1200), DMA(1201), I/O 모듈(1203), 마스크 ROM(1204), 불휘발성 메모리(1205), 작업 RAM(1206), 공개 키 암호화 모듈(1207), 공통 키 암호화 모듈(1208), 해쉬 함수 모듈(1209) 및 (진성) 난수 발생기(1210)를 포함하는 부정 변경이 어려운 하드웨어이다.

CPU(1200)는 부정 변경이 어려운 하드웨어의 개별 회로를 제어한다.

작업 RAM(1206)은 도 30에 도시된 작업 메모리(200)에 대응한다.

공개 키 암호화 모듈(1207)은 공개 키 암호 해독법에 따른 동작을 수행하는 데 사용되는데, 예를 들어 (1) 도 63에 도시된 SAM(105,)과 드라이브 CPU(1103)와의 상호 인증을 수행하고, (2) 매체 SAM(133a)의 서명 데이터를 생성하고 (EMD 서비스 센터(102), 콘텐츠 공급자(102) 및 제2 실시예에서는 서비스 공급자(310)와) 서명 데이터를 체크하고, (3) 전송될 소량의 데이터를 암호화 및 암호 해독화하고 (4) 상호 인증에 의해 얻어진 세션 키 데이터 K_{ses} 를 고유하는 데 사용된다. 공개 키 암호화 모듈(1107)은 회로 모듈(H/W IP 솔루션)로서 실시되거나 불휘발성 메모리(1205)에 저장된 공개 키 암호화 프로그램을 CPU(1200) (S/W IP 솔루션)에 의해 실행함으로써 실시될 수도 있다.

공통 키 암호화 모듈(1208)은 상호 인증을 수행하고, 상호 인증을 수행함으로써 얻어진 세션 키 데이터 K_{ses} 를 사용하여 키 파일 KF 및 KF_1 와 같은 데이터를 암호화 및 암호 해독화하는 데 사용된다. 공통 키 암호화 모듈(1108)은 회로 모듈(H/W IP 솔루션)로서 실시되거나 불휘발성 메모리(1205)에 저장된 공통 키 암호화 프로그램을 CPU(1200) (S/W IP 솔루션)에 의해 실행함으로써 실시될 수도 있다.

상호 인증은 공개 키 암호화 모듈(1207) 및 공통 키 암호화 모듈(1208)중 하나 또는 둘다에 의해 암호화 및 암호 해독화함으로써 실현될 수 있다.

해쉬 함수 모듈(1209)은 데이터의 해쉬 함수를 발생하는 데 사용된다. 특히, 해쉬 함수 모듈(1209)은 도 44a 내지 44d에 도시된 보안 콘텐츠이너(104x)의 키 파일 KF_1 의 해쉬값 H_{K1} 을 확인하는 데 사용된다. 해쉬 함수 모듈(1109)은 회로 모듈(H/W IP 솔루션)으로서 실시되거나 불휘발성 메모리(1205)에 저장된 해쉬 회로 모듈을 CPU(1200) (S/W IP 솔루션)에 의해 실행함으로써 실시될 수도 있다.

난수 발생기(1210)는 예를 들어 상호 인증을 수행하는 데 사용된다.

I/O 모듈(1203)은 도 63에 도시된 매체 SAM I/F(1007)와 통신하는 데 사용된다.

마스크 ROM(1204)은 출하될 때 매체 SAM(133)용의 초기화 프로그램 및 무결성 체크 프로그램과 같은 고정된 프로그램 및 데이터를 저장한다.

불휘발성 메모리(1205)는 암호화 프로그램 및 키 데이터와 같은 가변 프로그램을 저장한다.

도 74는 기록 매체(ROM)에 인스톨될 매체 SAM(133)을 출하할 때 마스크 ROM(1204) 및 불휘발성 메모리(1205)에 저장된다.

기록 매체(ROM)가 출하될 때, 도 74에서 도시된 바와 같이, 매체 SAM(133)에는 매체 SAM의 식별자(ID), 저장 키 데이터 K_{STR} (매체 키 데이터 K_{MED}), EMD 서비스 센터(102)의 공개 키 데이터 $K_{ESC,P}$, 근원 확인 기관(92)의 공개 키 데이터 $K_{R-CA,P}$, 매체 SAM(133)의 공개 키 확인 데이터 CER_{MSAM} , 매체 SAM(133)의 공개 키 데이터 $K_{MSAM,P}$, 매체 SAM(133)의 비밀 키 데이터 $K_{MSAM,S}$, 취소 리스트, 소유권 처리 데이터, 이익금을 수령하는 엔티 ID, 매체 유형 정보(매체 유형 정보 및 ROM 또는 RAM을 지정하는 정보), 키 파일 KF의 물리 어드레스 정보(레지스터 공간 어드레스), 각 콘텐츠 데이터 C의 키 파일 KF(콘텐츠 파일 CF), 및 소정의 체크값(MAC 값)이 저장되어 있다.

키 파일 KF의 물리 어드레스 정보(레지스터 공간 어드레스), 각 콘텐츠 데이터 C의 키 파일 KF(콘텐츠 파일 CF), 및 소정의 체크값(MAC 값)은 EMD 서비스 센터(102)에 의해 관리되는 허가 키 데이터 KD에 의해 암호화된다.

도 75는 기록 매체(ROM)에 설치될 매체 SAM(133)이 출하된 후 사용자 등록이 행해지고 구매 방식이 결정된 때의 마스크 ROM(1204) 및 불휘발성 메모리(1205)에 저장된 데이터를 예시한다.

도 75에서 도시된 바와 같이, 사용자 등록에 의해 매체 SAM(133)에 사용자 ID, 비밀 번호, 선호 정보, 설정 정보(예를 들어, 신용 카드 번호), 전자 화폐 정보, 키 파일 KF_1 , 등이 새로이 부가된다.

도 76에서는 기록 매체(ROM)에 설치될 매체 SAM(133)가 출하될 때의 마스크 ROM(1204) 및 불휘발성 메모리(1205)에 저장된 데이터를 예시한다.

기록 매체(ROM)가 출하될 때, 도 76에서 도시된 바와 같이, 매체 SAM(133)에는 매체 SAM의 식별자(ID), 저장 키 데이터 K_{STR} (매체 키 데이터 K_{MED}), EMD 서비스 센터(102)의 공개 키 데이터 $K_{ESC,P}$, 근원 확인 기관(92)의 공개 키 데이터 $K_{R-CA,P}$, 매체 SAM(133)의 공개 키 확인 데이터 CER_{MSAM} , 매체 SAM(133)의 공개 키 데이터 $K_{MSAM,P}$, 매체 SAM(133)의 비밀 키 데이터 $K_{MSAM,S}$, 취소 리스트, 소유권 처리 데이터, 이익금을 수령하는 엔티 ID, 및 매체 유형 정보(매체 유형 정보 및 ROM 또는 RAM을 지정하는 정보)가 저장되어 있다. 그러나, 키 파일 KF의 물리 어드레스 정보(레지스터 공간 어드레스), 각 콘텐츠 데이터 C의 키 파일 KF(콘텐츠 파일 CF), 및 소정의 체크값(MAC 값)은 저장되어 있지 않다.

도 77은 기록 매체(ROM)에 설치될 매체 SAM(133)가 출하된 후 사용자 등록이 행해지고 구매 방식이 결정된 때의 마스크 ROM(1204) 및 불휘발성 메모리(1205)에 저장된 데이터를 예시한다.

도 77에서 도시된 바와 같이, 사용자 등록에 의해 매체 SAM(133)에 사용자 ID, 비밀 번호, 선호 정보, 설정 정보(예를 들어, 신용 카드 번호), 전자 화폐 정보, 키 파일 KF의 물리 어드레스 정보(레지스터 공간 어드레스), 각 콘텐츠 데이터 C의 키 파일 KF(콘텐츠 파일 CF)의 키 파일 KF 및 KF_1 , 소정값(MAC 값) 등이 새로이 부가된다.

키 파일 KF의 물리 어드레스 정보(레지스터 공간 어드레스), 각 콘텐츠 데이터 C의 키 파일 KF(콘텐츠 파일 CF)의 키 파일 KF 및 KF_1 , 소정값(MAC 값)은 저장 키 데이터 K_{STR} 에 의해 암호화된다.

A/V 압축/압축 해제 SAM(163)

A/V 압축/압축 해제 SAM(163)은 예를 들어, 도 22에서 도시된 기능들을 구현한다.

도 78은 A/V 압축/압축 해제 SAM(163)의 회로 모듈을 예시한다.

A/V 압축/압축 해제 SAM(163)은 도 78에서 도시된 바와 같이 CPU/DSP(1300), DMA(1301), 마스크 ROM(1304), 불휘발성 메모리(1305), 작업 RAM(1306), 공통 키 암호화 모듈(1308), (진성) 난수 발생기(1310), 압축/압축 해제 모듈(1320), 디지털 워터마크 매립/검출 모듈(1321), 및 부분-정보 공개 제어 모듈(1322)을 포함하는 부정 변경 방지용(tamper-resistant) 하드웨어이다.

CPU/DSP(1300)는 예를 들어, 도 63에서 도시된 SAM(105₁)으로부터의 코멘드에 따라 마스크 ROM(1304) 및 불휘발성 메모리(1305)에 저장된 프로그램을 실행시킴으로써 A/V 압축/압축 해제 SAM(163) 내의 개별 회로 모듈들을 중앙 집중적으로 제어한다.

DMA(1301)는 마스크 ROM(1304), 불휘발성 메모리(1305), 및 작업 RAM(1306)에 대한 액세스를 CPU/DSP(1300)로부터의 코멘드에 따라 중앙 집중적으로 제어한다.

A/V 압축/압축 해제 SAM(163)이 출하될 때, 마스크 ROM(1304)에는 A/V 압축/압축 해제 SAM(163)에 대한 초기화 프로그램 및 무결성 체크 프로그램 등의 고정 프로그램과, A/V 압축/압축 해제 SAM(163)의 식별자 AVSAM_ID 등의 고정 데이터가 저장되어 있다.

불휘발성 메모리(1305)에는 암호화 프로그램 및 키 데이터 등의 변수 프로그램 및 데이터가 저장되어 있다.

작업 RAM(1306)에는 SAM(105)으로부터 수신된 키 파일 KF가 저장되어 있다.

공통 키 암호화 모듈(1308)은 상호 인증을 행하고 상호 인증에 의해 얻어진 세션 키 데이터 K_{SES}를 이용하여 콘텐츠 데이터 C 및 콘텐츠 키 데이터 Kc를 암호화하고 암호해제화하는 데 사용된다. 공통 키 암호화 모듈(1308)은 회로 모듈(H/W IP 솔루션)으로서 구현될 수 있거나 CPU/DSP(1300)에 의해 불휘발성 메모리(1305)에 저장된 공통 키 암호화 프로그램(S/W IP 솔루션)을 실행시켜 구현될 수 있다. 공통 키 암호화 모듈(1308)은 또한 SAM(105)으로부터 얻어진 콘텐츠 키 데이터 Kc를 이용하여 콘텐츠 데이터 C를 암호해제한다.

(진성) 난수 발생기(1310)는 예를 들어, SAM(105₁)와의 상호 인증을 행하는 데 사용된다.

압축/압축 해제 모듈(1320)은 예를 들어, 도 22에 도시된 압축 해제 유닛(223)의 기능들을 구현한다. 보다 상세히 기술하자면, 압축/압축 해제 모듈(1320)은 도 63에 도시된 충격 방지 메모리(1004) 및 다운로드 메모리(167)로부터 수신된 콘텐츠 데이터를 압축 해제하고, A/D 변환기로부터 수신된 콘텐츠 데이터를 압축한다.

디지털 워터마크 매핑/검출 모듈(1321)은 도 22에서 도시된 디지털 워터마크 정보 프로세서(224)의 기능들을 구현한다. 예를 들어, 디지털 워터마크 매핑/검출 모듈(1321)은 압축/압축 해제 모듈(1320)에서 처리되어질 콘텐츠 데이터에 소정의 디지털 워터마크 정보를 매핑시키고 콘텐츠 데이터에 매핑된 디지털 워터마크 정보를 검출, 즉 압축/압축 해제 모듈(1320)에서 실행된 처리가 적당함을 판단한다.

부분-정보 공개 제어 모듈(1322)은 도 22에서 도시된 부분적으로 공개하는 프로세서(225)를 구현하고, 재생 모드에 따라 콘텐츠 데이터를 재생한다.

매체 드라이브 SAM(260)

도 79는 매체 드라이브 SAM(260)의 회로 모듈을 예시한다.

매체 드라이브 SAM(260)는 도 79에서 도시된 마와 같이 CPU(1400), DMA(1401), 마스크 ROM(1404), 불휘발성 메모리(1405), 작업 RAM(1406), 공통 키 암호화 모듈(1408), 해쉬 함수 모듈(1409), (진성) 난수 발생기(1410), 엔코더/디코더 모듈(1420), 저장 키 데이터 생성 모듈(1430), 및 매체 고유 ID 생성 모듈(1440)을 포함하는 부정 변형 방지용 하드웨어이다.

CPU(1400)는 도 63에 도시된 드라이브 CPU(1003)로부터의 코멘드에 따라 마스크 ROM(1404) 및 불휘발성 메모리(1405)에 저장된 프로그램을 실행하여, 매체 드라이브 SAM(260) 내의 개별 회로 모듈들을 중앙 집중적으로 제어한다.

DMA(1401)는 마스크 ROM(1404), 불휘발성 메모리(1405), 및 작업 RAM(1406)에 대한 액세스를 CPU(1400)로부터의 코멘드에 따라 중앙 집중적으로 제어한다.

매체 드라이브 SAM(260)이 출하될 때, 마스크 ROM(1404)에는 매체 드라이브 SAM(260)에 대한 초기화 프로그램 및 무결성 체크 프로그램 등의 고정 프로그램과, 매체 드라이브 SAM(260)의 식별자 MDSAM_ID 등의 고정 데이터가 저장되어 있다.

불휘발성 메모리(1405)에는 암호화 프로그램 및 키 데이터 등의 변수 프로그램 및 데이터가 저장되어 있다.

작업 RAM(1406)은 각 중 처리를 실행하기 위한 작업 메모리로서 기능한다.

공통 키 암호화 모듈(1408)은 매체 SAM(133)과 A/V 압축/압해 모듈 SAM(163) 간에서의 상호 인증을 행하고 상호 인증에 의해 얻어진 공통 키인 세션 키 데이터 K_{SES} 를 이용하여 콘텐츠 파일 CF 및 키 파일 KF를 암호화 및 암호해제 하고, 또한 저장 키 데이터 K_{STR} 및 매체 키 데이터 K_{MED} 를 이용하여 콘텐츠 키 데이터 K_C 를 암호화하는 데 사용된다. 공통 키 암호화 모듈(1408)은 서명 데이터를 검증하여 서명 데이터가 생성되어질 데이터의 해쉬값과 공통 키 데이터를 이용하여 서명 데이터를 생성한다.

공통 키 암호화 모듈(1408)은 회로 모듈(H/W IP 솔루션)으로서 구현될 수 있거나 CPU(1400)에 의해 불휘발성 메모리(1405)에 저장된 공통 키 암호화 프로그램(S/W IP 솔루션)을 실행시켜 구현될 수 있다.

저장 키 데이터 K_{STR} 를 이용한 콘텐츠 키 데이터 K_C 에 대한 암호화를 매체 드라이브 SAM(260)의 공통 키 암호화 모듈(1408) 또는 매체 SAM 모듈(133)에 의해 행할 수 있다.

해쉬 함수 모듈(1409)은 서명 데이터를 검증하고 서명 데이터가 생성되어질 데이터의 해쉬값을 생성하는 데 사용된다.

(진성) 난수 발생기(1410)는 예를 들어, 매체 SAM(133)와의 상호 인증을 행하는 데 사용된다.

기록 매체(130)의 ROM 영역 또는 RAM 영역에 저장된 콘텐츠 데이터를 액세스할 때, 엔코더/디코더 모듈(1420)은 콘텐츠 데이터에 대해 엔코딩, 디코딩, ECC, 변조, 복조, 색터화, 및 디섹터화 등의 처리를 실행한다.

저장 키 데이터 생성 모듈(1430)은 매체 고유 ID 생성 모듈(1440)에서 생성된 매체 고유 ID를 이용하여 각 매체에 고유한 저장 키 데이터 K_{STR} 를 생성한다.

매체 고유 ID 생성 모듈(1440)은 매체 SAM(133)의 SAM_ID와 매체 드라이브 SAM(260)에 의해 생성된 드라이브 ID로부터 각 기록 매체에 고유한 매체 고유 ID를 생성한다.

도 1에서 도시된 EMD 시스템(100)의 전체 동작에 대해 도 80의 흐름도를 참조하면서 기술하기로 한다.

단계(S1)에서, 콘텐츠 공급자(101)가 소정의 등록을 행한 후, EMD 서비스 센터(102)는 콘텐츠 공급자(101)의 공개 키 데이터 $K_{CP,P}$ 의 공개 키 증명서 CER_{CP} 를 전송한다.

SAM(105₁ 내지 105₄)이 소정의 등록 처리를 행한 후, EMD 서비스 센터(102)는 또한 SAM(105₁ 내지 105₄)의 공개 키 데이터 $K_{SAM1,P}$ 내지 $K_{SAM4,P}$ 의 공개 키 증명서 CER_{CP1} 내지 CER_{CP4} 를 전송한다.

EMD 서비스 센터(102)는 상호 인증을 행한 후 1개월씩 유효한 3개월 동안 허가 키 데이터 KD_1 내지 KD_3 를 사용자 홈 네트워크(103)의 SAM(1051 내지 1054)에 전송한다.

이와 같은 방식으로, EMD 시스템(100)에서는, 허가 키 데이터 KD₁ 내지 KD₃가 SAM(105₁ 내지 105₄)에 사전에 분배된다. 이로써, SAM(105₁ 내지 105₄)은 비록 SAM(105₁ 내지 105₄)이 EMD 서비스 센터(102)와 분리되어 있을 때라도 콘텐츠 공급자(101)로부터 분배되어진 보안 컨테이너(104)를 구입하여 디코딩함으로써 보안 컨테이너(104)를 이용할 수 있다. 이 경우, 구입 및 이용 로그(usage log)는 이용 로그 데이터(108)에 기록되며, 이 데이터는 SAM(105₁ 내지 105₄)이 EMD 서비스 센터(102)에 접속될 때 자동적으로 EMD 서비스 센터(102)로 전송된다. 따라서, EMD 서비스 센터(102)는 설정 처리를 신뢰성있게 행할 수 있다. EMD 서비스 센터(102)가 이용 로그 데이터(108)를 소정 기간 동안 수신하지 않으면, 취소 리스트에서 해당하는 SAM을 무효로 만들 수 있다. 기본적으로는 SAM(105₁ 내지 105₄)로부터서 EMD 서비스 센터(102)로 UCS 데이터(166)가 실시간으로 전송된다.

단계(S2)에서, EMD 서비스 센터(102)와의 상호 인증을 행한 후, 콘텐츠 공급자(101)는 EMD 서비스 센터(102)에 UCP 데이터(106) 및 콘텐츠 키 데이터 Kc를 등록시킴으로써 이들 데이터를 인증한다. EMD 서비스 센터(102)는 또한 6개월 동안 키 파일 KF를 생성하여 이를 콘텐츠 공급자(101)에 전송한다.

단계(S3)에서, 콘텐츠 공급자(101)는 도 3a에서 도시된 콘텐츠 파일 CF 및 그에 대한 서명 데이터 SIG_{6,CP} 와, 도 3b에서 도시된 키 파일 KF 및 그에 대한 서명 데이터 SIG_{7,CP} 를 생성한다. 이어서, 콘텐츠 공급자(101)는 도 3c에서 도시된 상술된 파일 및 데이터와, 그에 대한 공개 키 증명서 데이터 CER_{CP} 및 서명 데이터 SIG_{1,ESC} 가 저장되어 있는 보안 컨테이너(104)를 사용자 홈 네트워크(103)의 SAM(105₁ 내지 105₄)에 온라인 또는 오프라인으로 전송한다.

보안 컨테이너(104)를 온라인으로 전송할 시에는, 콘텐츠 공급자(101)용 특정 프로토콜을 사용하여 그 프로토콜과는 독립적인 형태로(즉, 복수 계층으로 이루어진 통신 프로토콜을 사용하여 전송되어질 데이터) 콘텐츠 공급자(101)로부터 사용자 홈 네트워크(103)로 보안 컨테이너(104)를 분배한다. 보안 컨테이너(104)를 오프라인으로 전송할 시에는, 보안 컨테이너(104)를 기록 매체(ROM 또는 RAM)에 저장하여 컨테이너(101)로부터 사용자 홈 네트워크(103)로 전송한다.

다음, 단계 S4에서, 콘텐츠 파일 CF 및 키 파일 KF의 작성자 및 전송자의 정당성을 검증하기 위해 콘텐츠 제공자(101)로부터 분배된 안전 컨테이너(104) 내에서, 사용자 홈 네트워크(103)의 SAMs 105₁ 내지 105₄는 서명 데이터 SI G_{6,CP} , SIG_{7,CP} , 및 SIG_{1,ESC} 를 체크한다. 그로부터, SAMs 105₁ 내지 105₄는 해당 주기의 라이선스 키 데이터 KD₁ 내지 KD₆를 사용함에 의해 키 파일 KF를 암호해제한다.

다음, 단계 S5의 SAMs 105₁ 내지 105₄에서 구입 및 이용 모드는 도 22에서 도시된 동작 유닛(185) 상의 사용자 동작에 따라 주 CPU(810)로부터 내부 인터럽트 S810에 기초하여 결정된다.

이 경우에, 도 37에서 도시된 이용 모니터(186)는 안전 컨테이너(104)에 저장된 UCP 데이터(106) 상에 기초한 사용자에 의해 선택된 콘텐츠 파일 CF의 구입 및 이용 모드를 관리한다.

단계 S6에서, 도 37에서 도시된 SAMs 105₁ 내지 105₄의 회계 처리기(187)는 구입 및 이용 모드가 기록되는 이용 로그 데이터(108) 및 UCS 데이터(166)를 작성하며, 그것들을 EMD 서비스 센터(102)에 보낸다.

단계 S7에서, EMD 서비스 센터(102)는 이용 로그 데이터(108)에 기초하여 회계 처리를 실행하며, 결제 청구권 데이터(152) 및 결제 리포트 데이터(107)를 작성한다. EMD 서비스 센터(102)는 도 1에서 도시된 페이먼트 게이트웨이(90)를 거쳐서 결제 기관(91)에 그 대신 결제 청구권 데이터(152) 및 서명 데이터 SIG₉₉ 를 보낸다. EMD 서비스 센터(102)는 또한 콘텐츠 제공자에게 결제 리포트 데이터(107)를 보낸다.

다음, 단계 S8에서, 서명 데이터 SIG₉₉ 를 검증한 후에, 결제 기관(91)은 결제 리포트 데이터(152)에 기초하여, 사용자가 지불했던 금액을 콘텐츠 제공자(101)같은 그런 콘텐츠 권리 소유자에게 분배시킨다.

상술한 바와 같이, EMD 시스템(100)에서, 도 3a 내지 3c에서 도시된 안전 컨테이너(104)는 콘텐츠 제공자(101)로부터 사용자 홈 네트워크(103)까지 분배되며, 안전 컨테이너(104) 내의 키 파일 KF는 SAMs 105₁ 내지 105₄에서 처리된다.

키 파일 KF에 저장된 콘텐츠 키 데이터 Kc 및 UCP 데이터(106)는 라이선스 키 데이터 KD₁ 내지 KD₃를 이용해서 암호화되고, 라이선스 키 데이터 KD₁ 내지 KD₃를 보유하는 SAMs 105₁ 내지 105₄에서만 암호해제된다. SAMs 105₁ 내지 105₄는 콘텐츠 데이터 C의 구입 및 이용 모드가 UCP 데이터(106)에 기록되는 콘텐츠 데이터 C의 콘텐츠를 조경함에 기초하여 결정되는 잘 포장된(tamper-resistant) 하드웨어이다.

그러므로, EMD 시스템(100)에 따라, 콘텐츠 데이터 C는 신뢰성있게 구입될 수 있으며, 콘텐츠 제공자(101) 또는 콘텐츠 권리 소유자에 의해 작성된 UCP 데이터(106)에 기초하여 사용자 홈 네트워크(103)에서 이용될 수 있다.

게다가, EMD 시스템(100)에서, 콘텐츠 데이터 C는 안전 컨테이너(104)에서 그것을 저장함에 의해 콘텐츠 제공자(101)로부터 사용자 홈 네트워크(103) 온 라인 또는 오프라인까지 분배될 수 있다. 이 경우에, SAMs 105₁ 내지 105₄에서 콘텐츠 데이터 C의 권리 처리는 콘텐츠 데이터 C가 온라인 또는 오프라인에서 전송되었는 지에 의해 영향을 받지 않는다.

EMD 시스템(100)에서, 사용자 홈 네트워크(103)내의 네트워크 장치 160₁ 및 A/V 머신 160₂ 내지 160₄에서 콘텐츠 데이터 C를 전송, 기록, 이용, 구입에 있어, 처리는 항상 UCP 데이터(106)에 기초하여 실행된다. 이로써, 전체 사용자 홈 네트워크(103)에 보편적인 권리 처리 규칙이 설립될 수 있다.

도 81은 제1 실시예에서 이용된 안전 컨테이너(104)를 분배시키기 위한 프로토콜의 예를 도시한다.

다중 처리기 시스템(EMD 시스템: 100)에서 도 81에서 도시된 것과 같이, 콘텐츠 제공자(101)로부터 사용자 홈 네트워크(103)까지 안전 컨테이너(104)를 전달시키기 위한 프로토콜로서 예를 들면, TCP/IP 및 XML/SMIL이 사용된다.

사용자 홈 네트워크(103)의 SAM 상호간 또는 사용자 홈 네트워크(103 및 103a)간의 안전 컨테이너(104)를 전송하기 위한 프로토콜로서, 예를 들면, 1394 격렬 버스/인터페이스 상에 구현되는 XML/SMIL이 사용된다. 이 경우에, 안전 컨테이너(104)는 기록 매체(ROM 또는 RAM)에 저장될 수 있고 SAM 상호간에 분배될 수 있다.

< 제2 실시예>

제1 실시예에서, 콘텐츠 데이터는 콘텐츠 제공자(101)로부터 사용자 홈 네트워크(103)의 SAMs 105₁ 내지 105₄에 직접 분배된다. 제2 실시예에서, 콘텐츠 데이터는 콘텐츠 제공자로부터 서비스 제공자를 거쳐 사용자 홈 네트워크의 SAMs까지 분배된다.

도 82는 제2 실시예의 EMD 서비스 시스템(300)을 도시하는 블록도이다.

EMD 서비스 센터(300)는, 도 82에서 보여진 것과 같이, 콘텐츠 제공자(301), EMD 서비스 센터(302), 사용자 홈 네트워크(303), 서비스 제공자(310), 페이먼트 게이트웨이(90), 및 결제 기관(91)을 포함한다.

콘텐츠 제공자(301), EMD 서비스 센터(302), SAMs 305₁ 내지 305₄, 및 서비스 제공자(310) 각각은 본 발명의 데이터 제공 장치, 관리 장치, 데이터 처리 장치, 및 데이터 분배 장치에 해당한다.

콘텐츠 제공자(301)는 그것이 서비스 제공자(310)에게 콘텐츠 데이터를 공급한다는 것을 제외하고는 제1 실시예의 콘텐츠 제공자(101)와 유사하다.

EMD 서비스 센터(302)는 그것이 SAMs 305₁ 내지 305₄, 및 콘텐츠 제공자(101)에 대한 것 뿐만 아니라 서비스 제공자(301)에 대한 인증 기능, 키 데이터 관리 기능, 및 권리 처리 기능을 실행하는 것을 제외하고 제1 실시예의 EMD 서비스 센터(102)와 유사하다.

사용자 홈 네트워크(303)는 네트워크 장치(360₁) 및 A/V 머신(360₂ 내지 360₄)을 포함한다. 네트워크 장치(360₁)는 거기에 SAM(305₁) 및 CA 모듈(311)을 통합시키며, A/V 머신(360₂ 내지 360₄)은 거기에 SAM(305₂)를 통합시킨다.

SAMs 305₁ 내지 305₄는 그것들이 서비스 제공자(310)로부터 안전 컨테이너(304)를 수신하고, 콘텐츠 제공자(301) 및 서비스 제공자(310)의 서명 데이터를 검증하며, 또한 서비스 제공자(310)에 대한 서비스-제공자(SP) 구입 로그 데이터(데이터 분배 장치에 대한 데이터)를 작성한다는 점을 제외하고는 제1 실시예의 SAMs 105₁ 내지 105₄ 각각과 유사하다.

EMD 시스템(300)의 개요는 다음과 같다.

EMD 시스템(300)에서, 콘텐츠 제공자(301)는 제1 실시예의 것과 유사하고 제공될 것인 콘텐츠 데이터 C의 사용 허락 조건 등과 같은 그런 콘텐츠 데이터의 권리를 표시하는 콘텐츠 키 데이터 K_c 및 UCP 데이터(106)를 높은 신뢰성을 갖는 권위 기관이 있는 EMD 서비스 센터(302)에 전송한다. UCP 데이터(106) 및 콘텐츠 키 데이터 K_c는 EMD 서비스 센터(302)에 등록됨에 의해 권위화(인증)된다.

콘텐츠 제공자(301)는 콘텐츠 파일 CF를 작성하기 위해 콘텐츠 키 데이터 K_c로 콘텐츠 데이터 C를 암호화시킨다. 콘텐츠 제공자(301)는 EMD 서비스 센터(302)로부터 각 콘텐츠 파일 CF에 대해 6개월 동안 키 파일 KF를 수신한다.

키 파일 KF는 키 파일 KF의 정당성 및 키 파일 KF의 작성자 및 전송자의 정당성을 검증하기 위한 서명 데이터를 포함한다.

그리고 나서, 콘텐츠 제공자(301)는 콘텐츠 파일 CF, 키 파일 KF, 및 서명 데이터가 저장된 도 3a 내지 3c에 도시된 안전 컨테이너(104)를 기록 매체를 거친 오프라인 또는 인터넷 등의 네트워크, 디지털 방송을 거친 온 라인, 또는 비공식적인 프로토콜을 이용함에 의해 서비스 제공자(310)에게 공급한다.

안전 컨테이너(104)에 저장된 서명 데이터는 해당 데이터의 정당성과 그 데이터 작성자와 전송자의 정당성을 검증하기 위해 사용된다.

콘텐츠 제공자(301)로부터 안전 컨테이너(104)를 수신중에, 서비스 제공자(310)는 안전 컨테이너(104)의 작성자 및 전송자의 정당성을 검증하기 위해 서명 데이터를 체크한다.

다음에, 서비스 제공자(310)는 오프라인으로 서비스 제공자(310)에 리포트된 SRP에 저작 서비스 같은 그런 서비스 제공자(310)에 의해 부여된 서비스에 대한 가격을 가산함에 의해 얻어지거나, 콘텐츠 제공자(301)에 의해 요구된 가격 태그(tag) 데이터(PT:312)를 작성한다.

그리고 나서, 서비스 제공자(310)는 안전 컨테이너(104)로부터 콘텐츠 파일 CF 및 키 파일을 추출하고, 콘텐츠 파일 CF, 키 파일 KF, 가격 태그 데이터(312), 및 서명 데이터 K_{SP,S}가 거기에 저장되는 안전 컨테이너(304)를 작성한다.

키 파일 KF는 라이선스 키 데이터 KD₁ 내지 KD₆에 의해 암호화 되고, 서비스 제공자(310)가 라이선스 키 데이터 KD₁ 내지 KD₆를 소유하지 못하기 때문에, 그것은 키 파일 KF의 콘텐츠를 볼 수 없고 그것을 겹쳐줄 수 없다.

EMD 서비스 센터(302)는 또한 그것을 등록함에 의해 가격 태그 데이터(312)를 권위화 한다.

서비스 제공자(310)는 온 라인 또는 오프라인으로 사용자 홈 네트워크(303)에 안전 컨테이너(304)를 분배시킨다. 만약 안전 컨테이너가 오프라인으로 공급되면, 그것은 기록 매체(ROM)에 기록되거나 직접 SAMs 305₁ 내지 305₄에 공급된다. 만약 안전 컨테이너(304)가 온라인으로 공급되면, 서비스 제공자(310)는 우선 CA 모듈(311)과의 상호 인증을 행하고 세션(session) 키 데이터 K_{SES}를 이용하여 안전 컨테이너(304)를 암호화하여 전송한다. CA 모듈(311)은 암호화된 안전 컨테이너(304)를 수신하고 세션 키 데이터 K_{SES}를 이용하여 그것을 암호해제화하고 나서 SAMs 305₁ 내지 305₄에 그것을 전송한다.

이 경우에, 콘텐츠 제공자(301)로부터 사용자 홈 네트워크(303)에 안전 컨테이너(304)를 전송하기 위한 통신 프로토콜로서, MHEG는 디지털 방송에 대해 사용되고, XML/SMIL/HTML은 인터넷에 대해 사용된다. 안전 컨테이너(304)는 통신 프로토콜(코딩 방법)에 의존함이 없이 터널링 기술에 따라 해당 프로토콜에 내장된다.

따라서, 안전 컨테이너(304)의 포맷은 통신 프로토콜을 일치시킬 필요가 없어서, 안전 컨테이너(304)의 포맷을 선택함에 있어 유연성을 증가시킨다.

다음에, SAMs 305₁ 내지 305₄는 안전 컨테이너(304)에 저장된 콘텐츠 파일 CF 및 키 파일 KF의 전송자 및 작성자의 정당성을 검증하기 위해 안전 컨테이너(304)에 저장된 서명 데이터를 체크한다. 그리고 나서, SAM 305₁ 내지 305₄는 EMD 서비스 센터(302)로부터 분배된 해당 주기의 라이선스 키 데이터 KD₁ 내지 KD₃를 이용하여 키 파일 KF를 암호해제한다.

네트워크 장치(360₁) 및 A/V 머신(360₂ 내지 360₄)에 있어서, SAMs 305₁ 내지 305₄에 공급된 안전 컨테이너(304)의 구입 및 이용 모드는 사용자 동작에 따라 결정되며, 그리고 나서 안전 컨테이너(304)는 재생되거나 기록 매체에 기록될 준비가 되어 있다.

SAMs 305₁ 내지 305₄는 이용 로그 데이터(308)로서 안전 컨테이너(304)의 구입 및 이용 로그를 기록한다. 이용 로그 데이터(308)는, 예를 들면, EMD 서비스 센터(302)로부터의 요구에 응하여 사용자 홈 네트워크(303)로부터 EMD 서비스 센터(302)에 전송된다.

SAMs 305₁ 내지 305₄는, 콘텐츠의 구입 모드를 결정하면, 구입 모드를 표시하는 UCS 데이터(166)를 EMD 서비스 센터(302)에 전송한다.

EMD 서비스 센터(302)는 이용 로그 데이터(308)에 기초하여 콘텐츠 제공자(301) 및 서비스 제공자(310) 각각에 대한 회계 콘텐츠를 결정하고(계산하고), 계산된 회계 콘텐츠에 기초하여 페이먼트 게이트웨이(90)를 거쳐 은행등의 결제 기관(91)에 결제를 한다. 이 결제에 따라, 사용자 홈 네트워크(303)의 사용자가 결제 기관(91)에 지불한 금액이 EMD 서비스 센터(302)에 의해 수행된 결제 처리에 의해 콘텐츠 제공자(301) 및 서비스 제공자(310)에게 주어진다.

이 실시예에서, EMD 서비스 센터(302)는 인증 기능, 키 데이터 관리 기능, 및 권리 처리(이익 분배) 기능을 가진다.

좀 더 구체적으로, EMD 서비스 센터(302)는 중립의 입장에 있는 최고 권위 기관인 루트(root) 인증국(92)보다 한 단계 낮은 곳에 위치한 제2 인증국으로서의 역할을 하며, EMD 서비스 센터(102)의 비밀 키 데이터를 사용하여 공개 키 데이터의 공개 키 증명 데이터에 서명을 붙여 공개 키 데이터를 인증한다. 공개 키 데이터는 콘텐츠 제공자(301), 서비스 제공자(310), 및 SAMs 305₁ 내지 305₄에 있어 서명 데이터의 정당성을 검증하기 위해 사용된다. 상술한 바와 같이, EMD 서비스 센터(102)가 콘텐츠 제공자(301)의 UCP 데이터(106), 콘텐츠 키 데이터 Kc, 및 서비스 제공자(310)의 가격 태그 데이터(312)를 등록하여 권위화 하는 것도 또한 EMD 서비스 센터(302)의 인증 기능에 따른 것이다.

EMD 서비스 센터(302)는 또한 라이선스 키 데이터 KD₁ 내지 KD₆와 같은 그런 키 데이터를 관리하는 키 - 데이터 관리 기능을 가지고 있다.

EMD 서비스 센터(302)는 또한 다음의 권리 처리(이익 분배) 기능을 가지고 있다. EMD 서비스 센터(302)는 콘텐츠 제공자(301)에 의해 등록된 UCP 데이터(106), SAMs 305₁ 내지 305₄로부터 입력된 이용 로그 데이터(308), 및 서비스 제공자에 의해 등록된 가격 태그 데이터(312)에 기초하여 사용자가 의해 콘텐츠의 구입 및 이용에 대해 결제를 행하고, 사용자가 지불한 금액을 콘텐츠 제공자(301) 및 서비스 제공자(310)에게 분배시킨다.

콘텐츠 제공자(301)의 각 구성 요소에 대해 상세하게 설명하면 다음과 같다.

[콘텐츠 제공자(301)]

콘텐츠 제공자(301)는 그것이 도 3a 내지 3c에서 도시된 안전 컨테이너(104)를 온라인 또는 오프라인으로 서비스 제공자(310)에 공급한다는 점을 제외하고는 제1 실시예의 콘텐츠 제공자(101)와 유사하다.

즉, 콘텐츠 제공자(301)는 도 17 내지 19에서 도시된 처리에 따라 안전 컨테이너(104)를 작성하고 그것을 콘텐츠 제공자를 위한 프로토콜을 분배시키는 산물에 삽입한다.

다음에, 서비스 제공자(310)는 안전 컨테이너(104)를 다운로드 하고 프로토콜로부터 그것을 추출한다.

[서비스 제공자(310)]

서비스 제공자(310)는 콘텐츠 제공자(301) 및 가격 태그 데이터(312)로부터 공급된 콘텐츠 파일 CF 및 키 파일 KF가 저장되는 안전 컨테이너(304)를 작성하고, 온라인 또는 오프라인으로 사용자 홈 네트워크(303)의 네트워크 장치(360₁) 및 A/V 머신 360₂ 내지 360₄에 그것을 분배시킨다.

서비스 제공자(310)에 따른 콘텐츠 배급의 서비스 형태에는 크게 둘로 나누어 독립형 서비스와 종속형 서비스가 있다.

독립형 서비스는 개별적으로 콘텐츠를 분배시키기 위한 다운로드 서비스이다. 종속형 서비스는 프로그램 또는 광고(CM)와 함께 콘텐츠를 분배시키기 위한 서비스이며, 예를 들면, 드라마 프로그램 스트림(stream) 내에 드라마 프로그램의 주제가를 삽입함에 의해 주제가 콘텐츠를 공급하는 것이 해당된다. 이것은 사용자가 드라마 프로그램을 시청하는 동안 스트림내에 저장된 콘텐츠를 구입하게 한다.

서비스 제공자(310)는 콘텐츠 제공자(301)로부터 안전 컨테이너(104)의 제공을 수신하면, 이하의 처리에 따라 안전 컨테이너(304)를 작성한다.

이하, 콘텐츠 제공자(301)로부터 수신된 안전 컨테이너(104)로부터 안전 컨테이너(304)를 작성하고 그것을 사용자 홈 네트워크(303)에 분배시키기 위한 처리를 도 83의 흐름도를 참조하여 설명될 것이다.

단계 S83-1에서, 서비스 제공자(310)는 온라인 또는 오프라인으로 콘텐츠 제공자(301)로부터 도 3a 내지 3c에 도시된 안전 컨테이너(104)를 수신하고, 그것을 저장한다.

단약 안전 컨테이너(104)가 온라인으로 보내지면, 안전 컨테이너(104)는 콘텐츠 제공자(301)와 서비스 제공자(310)간의 상호 인증에 의해 취득된 세션 키 데이터 K_{SES}를 사용함에 의해 암호해제된다.

단계 S83-2에서, 서비스 제공자(310)는 EMD 서비스 센터(302)의 공개 키 데이터 K_{ESC,P}를 사용하여 안전 컨테이너(104)의 도 3c에서 도시된 서명 데이터 SIG_{1,ESC}의 정당성을 검증하고 나서 도 3c에서 도시된 공개 키 증명 데이터 CER_{CP}로부터 공개 키 데이터 K_{CP,P}를 추출한다.

다음에, 서비스 제공자(310)는 키 파일 KF의 전송자 및 콘텐츠 파일 CF의 전송자 및 작성자의 정당성을 검증하기 위해, 추출된 공개 키 데이터 K_{CP,P}를 사용하여 도 3a 및 3b 각각에 도시된 안전 컨테이너(104)의 서명 데이터 SIG₆, CP 및 SIG_{7,CP}를 체크한다.

서비스 제공자(310)는 또한 키 파일 KF 작성자의 정당성을 검증하기 위해 공개 키 데이터 K_{ESC,P}를 사용하여 도 3b에서 도시된 키 파일 KF 내에 저장된 서명 데이터 SIG_{K1,ESC}를 체크한다. 이것은 또한 EMD 서비스 센터(102)에서 키 파일의 공식적 등록을 검증한다.

이하, 단계 S83-3에서, 서비스 제공자(310)는 서비스 제공자(310)의 서비스에 대한 가격을 오프라인으로 콘텐츠 제공자(301)로부터 보고되었던 콘텐츠 제공자(301)가 원하는 RSP에 가산하여 취득된 가격 태그 데이터(312)를 작성한다.

또한 서비스 프로바이더(310)는 서비스 프로바이더(310)의 비밀 키 데이터(K_{SP,P})를 사용함으로써, 콘텐츠 파일(CF), 키 파일(KF), 및 프라이스 태그 데이터(312)의 해쉬 값으로부터 각각 서명 데이터(SIG_{62,SP}, SIG_{63,SP} 및 SIG_{64,SP})를 생성시킨다.

서명 데이터(SIG_{62,SP})는 콘텐츠 파일(CF)의 센터의 정당성을 검증하기 위해 사용되고, 서명 데이터(SIG_{63,SP})는 키 파일(KF)의 센터를 검증하기 위해 사용되고, 서명 데이터(SIG_{64,SP})는 프라이스 태그 데이터(312)의 생성기 및 센터를 검증하기 위해 사용된다.

다음으로, 서비스 프로바이더(310)는 도 84a에 도시된 콘텐츠 파일(CF) 및 그 서명 데이터(SIG_{6,CP}, SIG_{62,SP}), 도 84b에 도시된 키 파일(KF) 및 그 서명 데이터(SIG_{7,CP}, SIG_{63,ESC}), 도 84c에 도시된 프라이스 태그 데이터(312) 및 그 서명 데이터(SIG_{64,SP}), 도 84d에 도시된 공개 키 증명 데이터(CER_{SP}) 및 그 서명 데이터(SIG_{61,ESC}) 및 증명 데이터(CER_{CP}) 및 그 서명 데이터(SIG_{1,ESC})가 저장된 시큐어 컨테이너(304)를 생성하고, 생성된 시큐어 컨테이너(304)를 시큐어 컨테이너 데이터베이스에 저장한다.

시큐어 컨테이너 데이터베이스에 저장된 시큐어 컨테이너(304)는 일례로 콘텐츠 ID를 사용함으로써 서비스 프로바이더(310)에 의해 일원적으로 관리된다.

도 84a는 DSP가 콘텐츠 데이터(C)를 압축 해제하는 A/V 압축/압축 해제 디바이스로서 사용되는 경우의 콘텐츠 파일(CF)의 구성을 도시한다. 해당 DSP에서는, 시큐어 컨테이너(304) 내의 A/V 압축 해제 소프트웨어 및 디지털 워터마크 정보 모듈을 이용하여, 시큐어 컨테이너(304) 내의 콘텐츠 데이터(C)의 압축 해제 및 디지털 워터마크 정보를 매입하고(embed) 검출한다. 그 때문에, 콘텐츠 프로바이더(301)는 임의의 압축 방법 및 디지털 워터마크 정보가 매입 방법을 채용할 수 있다.

AV 압축/압축 해제 디바이스로서 콘텐츠 데이터(C)를 압축 해제하고 디지털 워터마크 정보의 매입하고 검출하는 하드웨어 또는 미리 저장된 소프트웨어를 이용하는 경우에는, 콘텐츠 파일(CF) 내에 A/V 압축 해제 소프트웨어 및 디지털 워터마크 정보 모듈을 저장하지 않을 수도 있다.

단계 S83-4에서, 서비스 프로바이더(310)는, 사용자 홈 네트워크(303)로부터의 요구에 따라 시큐어 컨테이너(304)를 시큐어 컨테이너 데이터베이스로부터 판독한다.

이 때, 시큐어 컨테이너(304)는, 복수의 콘텐츠 파일(CF) 및 이들에 각각 대응한 복수의 키 파일(KF)를 저장한 복합 컨테이너일 수 있다. 예를 들면, 각각 곡, 비디오클립, 워드 카드, 라이너 노트 및 챗킷에 관한 복수의 콘텐츠 파일(CF)을 단일 시큐어 컨테이너(304)에 저장할 수 있다. 이것들의 복수의 콘텐츠 파일(CF) 등은, 디렉토리 구조로 시큐어 컨테이너(304) 내에 저장할 수 있다.

시큐어 컨테이너(304)가, 디지털방송을 통하여 송신되는 경우에는, MHEG 프로토콜이 채용된다. 시큐어 컨테이너(304)가, 인터넷으로 송신되는 경우에는 XML/SMIL/HTML 프로토콜이 채용된다.

이 때, 시큐어 컨테이너(304) 내의 콘텐츠 파일(CF) 및 키 파일(KF) 등은, MHEG 및 HTML 프로토콜 같은 코딩 방법에 의존하지 않은 형식으로, 서비스 프로바이더(310)와 사용자 홈 네트워크(303)와의 사이에서 채용되는 통신 프로토콜 내의 소정의 층에 저장된다.

예를 들면, 시큐어 컨테이너(304)를 디지털 방송을 통하여 송신되는 경우에는, 도 85에 도시한 바와 같이, 콘텐츠 파일(CF)이, MHEG 오브젝트(object) 내의 MHEG 콘텐츠 데이터로서 저장된다.

또한, MHEG 오브젝트는, 동화상인 경우에는 트랜스포트 층 프로토콜 내의 PES(Packetized Elementary Stream) - 비디오에 저장되고, 음성인 경우에는 트랜스포트 층 프로토콜 내의 PES - 오디오에 저장되며, 정지 화상인 경우에는 프라이빗 데이터(Private - Data)에 저장된다.

도 86에 도시한 바와 같이, 키 파일(KF), 프라이스 태그 데이터(312) 및 공개 키 증명 데이터(CER_{CP}, CER_{SP})는, 트랜스포트 층 프로토콜의 TS 패킷 내의 ECM(Entitlement Control Message)에 저장된다.

콘텐츠 파일(CF), 키 파일(KF), 프라이스 태그 데이터(312) 및 공개 키 증명 데이터(CER_{CP}, CER_{SP})는, 콘텐츠 파일(CF)의 헤더 내의 디렉토리 구조 데이터(DSD₁)에 의해서 상호간의 링크가 확립되어 있다.

다음에, 서비스 프로바이더(310)는, 시큐어 컨테이너(304)를 오프 라인 및/또는 온라인으로 사용자 홈 네트워크(303)에 공급한다.

시큐어 컨테이너(304)가 온라인으로 사용자 홈 네트워크(303)의 네트워크 기기(360₁)에 발급되는 경우에는, 서비스 프로바이더(310)는, 상호인증 후에, 세션 키 데이터(K_{SES})를 이용하여 시큐어 컨테이너(304)를 암호화한 후에, 네트워크를 통해 네트워크 기기(360₁)에 발급한다.

시큐어 컨테이너(304)를 위성을 통해 방송하는 경우에는, 서비스 프로바이더(310)는, 시큐어 컨테이너(304)를 스크램블 키 데이터(K_{SCR})를 이용하여 암호화한다. 또한, 스크램블 키 데이터(K_{SCR})가 워크 키 데이터(K_w)에 의해 암호화되고, 워크 키 데이터(K_w)가 마스터 키 데이터(K_M)을 이용하여 암호화된다.

그리고, 서비스 프로바이더(310)는, 시큐어 컨테이너(304)와 함께, 스크램블 키 데이터(K_{SCR}) 및 워크 키 데이터(K_w)를, 위성을 통해 사용자 홈 네트워크(303)에 송신한다. 또한, 서비스 프로바이더(310)는, 마스터 키 데이터(K_M)을, 예를 들면, IC 카드 등에 기억시켜서 오프 라인에서 사용자 홈 네트워크(303)에 발급한다.

사용자 홈 네트워크(303)로부터, 콘텐츠 데이터(C)에 관한 SP 구입 이력 데이터(SP purchase log data) (309)를 수신한 후에, 서비스 프로바이더(310)는 이것을 저장한다.

장래의 서비스 콘텐츠즈를 결정할 때에, 서비스 프로바이더(310)는, SP 구입 이력 데이터(309)를 참조한다. 또한, 서비스 프로바이더(310)는, SP 구입 이력 데이터(309)에 기초하여, 해당 SP 구입 이력 데이터(309)를 송신한 SAM(305₁~305₄)의 사용자의 기호를 분석하여 사용자 기호 필터 데이터(900)를 생성하여, 이것을 사용자 홈 네트워크(303)의 CA 모듈(311)에 송신한다.

서비스 프로바이더(310) 및 서비스 프로바이더(310)의 관계자는, 서비스 프로바이더(310)의 신분증명서 및 결제 처리를 행하는 은행 계좌 등을 이용하여, 오프 라인에서, EMD 서비스센터(302)에 등록 처리를 행하고, 글로벌적으로 고유한 식별자 SP_ID를 얻고 있다.

또한, 서비스 프로바이더(310)는, EMD 서비스센터(302)에 프라이스 태그 데이터(312)를 등록하여 권위화한다(authorize).

< EMD 서비스센터(302) >

상술한 바와 같이, EMD 서비스센터(302)는, 인증국(CA: Certificate Authority), 키 관리(Key Management)국 및 권리 처리(Rights Clearing)국으로서의 역할을 완수한다.

도 87는, EMD 서비스센터(302)의 주된 기능을 도시한 도면이다. 도 87에 도시한 바와 같이, EMD 서비스센터(302)는, 주로, 라이선스 키 데이터를 콘텐츠 프로바이더(301) 및 SAM(305₁~305₄)에 공급하는 처리와, 공개 키 증명 데이터(CER_{CP}, CER_{SP}, 및 CER_{SAM1}~CER_{SAM4})의 발행 처리와, 키 파일(KF)의 생성 처리, 이용 이력 데이터(308)에 기초를 둔 결제 처리(이익분배 처리)를 행한다.

여기서, 라이선스 키 데이터의 공급 처리와, 공개 키 증명 데이터(CER_{CP}, 및 CER_{SAM1}~CER_{SAM4})의 발행 처리와, 키 파일(KF)의 생성 처리는 제1 실시예의 EMD 서비스센터(102)와 동일하다.

그러나, EMD 서비스센터(302)는, EMD 서비스센터(102)와는 달리, 서비스 프로바이더(310)의 공개 키 증명 데이터(CER_{SP})의 발행 처리를 행하고, 또한, 이용 이력 데이터(308)에 기초하여, SAM(305₁~305₄)에 있어서의 콘텐츠 데이터(C)의 구입에 의해서 지불된 이익을 콘텐츠 프로바이더(301), 콘텐츠 프로바이더의 관계자, 서비스 프로바이더(310), 및 서비스 프로바이더의 관계자에게 분배하는 이익분배 처리를 행한다.

이용 이력 데이터(308)의 콘텐츠는 도 21에 도시된 것일 수 있다.

또한, EMD 서비스센터(302)는, 이용 이력 데이터(308)에 기초하여, 해당 이용 이력 데이터(308)를 송신한 SAM(305₁~305₄)의 사용자의 기호에 따라 콘텐츠 데이터(C)를 선택하기 위한 사용자 기호 필터 데이터(900)를 생성하여, 사용자 기호 필터 데이터(900)를 SAM 관리부(149)를 통해, 해당 이용 이력 데이터(308)를 송신한 SAM(305₁~305₄)에 송신한다.

< 사용자 홈 네트워크(303) >

사용자 홈 네트워크(303)는, 도 82에 도시한 바와 같이, 네트워크 기기(360₁) 및 A/V 기기(360₂~360₄)를 갖고 있다.

네트워크 기기(360₁)는, CA 모듈(311) 및 SAM(305₁)을 내장하고 있다. 또한, AV 기기(360₂~360₄)는, 각각 S AM(305₂~305₄)을 내장하고 있다.

SAM(305₁~305₄)의 상호간은, 예를 들면, 1394 직렬 인터페이스 버스 등의 버스(191)를 통해 접속되어 있다.

또, AV 기기(360₂~360₄)는, 네트워크 통신 기능을 갖고 있을 수 있지만 중요한 것은 아니다. 네트워크 통신 기능이 제공되지 않는 경우, AV 기기(360₂~360₄)는, 버스(191)를 통해 네트워크 기기(360₁)의 네트워크 통신 기능을 간단히 이용할 수 있다. 대안으로서, 사용자 홈 네트워크(303)는, 네트워크 기능을 갖고 있지 않은 AV 기기만을 갖고 있을 수도 있다.

이하, 네트워크 기기(360₁)에 관해서 설명한다.

도 88는, 네트워크 기기(360₁)의 구성도이다. 도 88에 도시한 바와 같이, 네트워크 기기(360₁)는, 통신 모듈(162), CA 모듈(311), 디코딩 모듈(905), SAM(3051), AV 압축/압축 해제 SAM(163), 조작부(165), 다운로드 메모리(167), 재생 모듈(169), 외부 메모리(201) 및 호스트 CPU(810)를 갖는다. 도 22와 동일 부호를 붙인 구성 요소는, 동일 참조 번호로 표시된다.

통신 모듈(162)은, 서비스 프로바이더(310)와의 통신 처리를 행한다. 구체적으로는, 통신 모듈(162)은, 서비스 프로바이더(310)로부터 위성 방송 등을 통하여 수신한 시큐어 컨테이너(304)를 디코딩 모듈(905)에 출력한다. 또한, 통신 모듈(162)은, 서비스 프로바이더(310)로부터 전화 회선 등을 통해 수신한 사용자 기호 필터 데이터(900)를 CA 모듈(311)에 출력함과 함께, CA 모듈(311)로부터 수신한 SP 구입 이력 데이터(309)를 전화 회선 등을 통해 서비스 프로바이더(310)에 송신한다.

도 89는, CA 모듈(311) 및 디코딩 모듈(905)의 기능 블록도이다.

도 89에 도시한 바와 같이, CA 모듈(311)은, 상호인증부(906), 기억부(907), 암호화/암호해제화부(908) 및 SP 구입 이력 데이터 생성부(909)를 갖는다.

CA 모듈(311)과 서비스 프로바이더(310)와의 사이에서 전화 회선을 통해 데이터를 송수신할 때에, 상호인증부(906)는 서비스 프로바이더(310)와의 사이에서 상호인증을 행하여 세션 키 데이터(K_{SES})를 생성하고, 이것을 암호화/암호 해제화부(908)에 출력한다.

기억부(907)는, 서비스 프로바이더(310)와 사용자와의 사이에서 계약이 성립한 후에, 서비스 프로바이더(310)로부터 IC 카드(912) 등을 이용하여 오프 라인으로 공급된 마스터 키 데이터(K_M)를 기억한다.

암호화/암호해제화부(908)는, 디코딩 모듈(905)의 디코더(910)로부터 각각 암호화된 스크램블 키 데이터(K_{SCR}) 및 워크 키 데이터(K_W)를 수신하고, 기억부(907)로부터 판독한 마스터 키 데이터(K_M)을 이용하여 워크 키 데이터(K_W)를 암호해제한다. 그리고, 암호화/암호해제화부(908)는, 해당 암호해제한 워크 키 데이터(K_W)를 이용하여 스크램블 키 데이터(K_{SCR})를 암호해제하고, 해당 암호해제한 스크램블 키 데이터(K_{SCR})를 암호해제부(910)에 출력한다.

또한, 암호화/암호해제화부(908)는, 전화 회선 등을 통해 통신 모듈(162)이 서비스 프로바이더(310)로부터 수신한 사용자 기호 필터 데이터(900)를, 상호인증부(906)로부터의 세션 키 데이터(K_{SES})를 이용하여 암호해제하고, 디코딩 모듈(905)의 시큐어 컨테이너 선택부(911)에 출력한다.

암호화/암호해제화부(908)는, SP 구입 이력 데이터 생성부(909)로부터 수신한 SP 구입 이력 데이터(309)를, 상호인증부(906)로부터의 세션 키 데이터(K_{SES})를 이용하여 암호해제하고, 통신 모듈(162)을 통해 서버사 프로바이더(310)에 송신한다.

SP 구입 이력 데이터 생성부(909)는, 도 88에 도시한 조작부(165) 상의 사용자 조작을 이행함으로써 얻어진 조작 신호(S165), 또는 SAM(305₁)으로부터의 UCS 데이터(166)에 기초하여, 서비스 프로바이더(310)에 고유의 콘텐츠 데이터(C)의 구입 이력을 표시하는 SP 구입 이력 데이터(309)를 생성한다. 이어서 SP 구입 이력 데이터 생성부(909)는, SP 구입 이력 데이터(309)를 암호화/암호해제화부(908)에 출력한다.

SP 구입 이력 데이터(309)는, 예를 들면, 사용자의 의견을 반영한 서비스 프로바이더(310)의 배급 서비스에 관한 정보, 매월 기본 요금(네트워크 요금), 계약(갱신) 정보 및 구입 이력 정보 등을 포함한다.

또, CA 모듈(311)은, 서비스 프로바이더(310)가 회계 기능(accounting function)을 갖고 있는 경우에는, 서비스 프로바이더(310)의 회계 데이터 베이스(account data base), 고객 관리 데이터 베이스 및 마케팅 정보 데이터 베이스와 통신을 행한다. 이 경우에, CA 모듈(311)은, 콘텐츠 데이터의 배급 서비스에 관한 회계 데이터를 서비스 프로바이더(310)에 송신한다.

디코딩 모듈(905)은, 디코더(910) 및 시큐어 컨테이너 선택부(911)을 갖는다.

디코더(910)는, 통신 모듈(162)로부터, 각각 암호화된 시큐어 컨테이너(304), 스크램블 키 데이터(K_{SCR}) 및 워크 키 데이터(K_W)를 수신한다. 그리고, 디코더(910)는, 암호화된 스크램블 키 데이터(K_{SCR}) 및 워크 키 데이터(K_W)를 CA 모듈(311)의 암호화/암호해제화부(908)에 출력하고 암호화/암호해제부(908)로부터 암호해제화된 스크램블 키 데이터(K_{SCR})를 수신한다. 또한, 디코더(910)는, 암호화된 시큐어 컨테이너(304)를, 스크램블 키 데이터(K_{SCR})를 이용하여 암호해제한 후에, 시큐어 컨테이너 선택부(911)에 출력한다.

또, 시큐어 컨테이너(304)가, MPEG2 전송 스트림 방법에 따라 서비스 프로바이더(310)로부터 송신되는 경우에는, 디코더(910)는, TS 패킷 내의 ECM로부터 스크램블 키 데이터(K_{SCR})를 추출하고, EMM으로부터 워크 키 데이터(K_W)를 추출한다.

또한, ECM에는, 채널마다의 프로그램 속성 정보 등이 포함되고 있다. 또한, EMM은, 사용자(시청자)마다 다른 개별 시청계약 정보 등이 포함되고 있다.

시큐어 컨테이너 선택부(911), 디코더(910)로부터 수신된 시큐어 컨테이너(304)를, CA 모듈(311)로부터 수신된 사용자 기호 필터 데이터(900)를 이용하여 필터링 처리하여, 사용자의 기호에 따른 시큐어 컨테이너(304)를 선택하여 SAM(305₁)에 출력한다.

다음에, SAM(305₁)에 관해서 설명한다.

또, SAM(305₁)는, 서비스 프로바이더(310)에 관한 서명 검증 처리를 행하는 등, 콘텐츠 프로바이더(301) 외에 서비스 프로바이더(310)에 관하여도 처리를 행하는 점을 제외하고, 도 22~도 72등을 이용하여 전술한 제1 실시예의 SAM(105₁)와 기본적으로 유사한 기능 및 구조를 갖고 있다.

SAM(305₁~305₄)는, 콘텐츠 단위의 회계 처리를 행하는 모듈이고, EMD 서비스센터(302)와의 사이에서 통신을 행한다.

또한, 도 63에 도시하는 구성은 사용자 홈 네트워크(303) 내의 기기에 있어서도 적용 가능하다. 또한, 도 68~도 79을 이용하여 설명한 권리 처리 SAM, 미디어 SAM(133), AV 압축/압축 해제 SAM(163) 및 미디어 구동 SAM(260)의 구성은, 사용자 홈 네트워크(303) 내의 기기로 이용되는 각종의 SAM(305₁~305₄)에도 적용된다.

또한, SAM(305₂~305₄)은, SAM(305₁)과 기본적으로 동일 기능을 갖는다.

이하, SAM(3051)의 기능에 관해서 상세히 설명한다.

도 90은, SAM(305₁)의 기능의 구성도이며, 또한, 서비스 프로바이더(310)로부터 시큐어 컨테이너(304)를 수신할 때의 처리에 관련하는 데이터의 흐름이 도시되고 있다.

도 90에 도시한 바와 같이, SAM(305₁)는, 상호인증부(170), 암호화/암호해제부(171, 172, 173), 다운로드 메모리 관리부(182), AV 압축/압축 해제 SAM 관리부(184), EMD 서비스센터 관리부(185), 이용 감시부(186), SAM 관리부(190), 기억부(192), 미디어 SAM 관리부(197), 작업용 메모리(200), 서비스 프로바이더 관리부(580), 회계 처리부(587), 서명 처리부(589), 외부 메모리 관리부(811) 및 CPU(1100)를 갖는다.

또, SAM(105₁)의 경우와 마찬가지로, 도 90에 도시하는 SAM(305₁)의 소정의 기능은, CPU에 의해 프라이빗 프로그램을 실행함으로써 실현된다.

도 90에 있어서, 도 30 등과 동일 부호를 붙인 기능 블록은, 제1 실시예로 설명한 동일 부호의 기능 블록과 동일하다.

도 88에 도시하는 외부 메모리(201)에는, 제1 실시예에 설명한 처리 및 후술하는 처리를 실행함으로써 이용 이력 데이터(308) 및 SAM 등록 리스트가 기억된다.

또한, 작업용 메모리(200)에는, 도 91에 도시한 바와 같이, 콘텐츠 키 데이터(Kc), UCP 데이터(106), 기억부(192)의 로크 키 데이터(K_{LOC}), 콘텐츠 프로바이더(301)의 공개 키 증명 데이터(CER_{CP}), 서비스 프로바이더(310)의 공개 키 증명 데이터(CER_{SP}), UCS 데이터(366), SAM 프로그램 다운로드 컨테이너(SDC1~SDC3) 및 프라이스 태그 데이터(312) 등이 기억된다.

이하, SAM(305₁)의 기능 블록 중, 도 90의 제2 실시예에 있어서 고유한 기능 블록만에 관해서 설명한다.

서명 처리부(589)는, 기억부(192) 또는 작업용 메모리(200)로부터 판독한 EMD 서비스센터(302)의 공개 키 데이터(K_{ESC,P}), 콘텐츠 프로바이더(301)의 공개 키 데이터(K_{CP,P}) 및 서비스 프로바이더(310)의 공개 키 데이터(K_{SP,P})를 이용하여, 시큐어 컨테이너(304) 내의 서명 데이터의 검증을 행한다.

CPU(1100)가 도 92에 도시한 바와 같이 사용자의 조작에 따라 호스트 CPU(810)로부터 내부 인터럽트(S810)를 수신할 때, 과금 처리기(587)는 작업 메모리(200)으로부터 판독한 가격표 데이터(312)에 근거하여 콘텐츠의 구매 및 그 콘텐츠의 사용 모드에 따라 CPU(1100)의 제어하에서 과금 처리를 수행한다.

사용자에게 콘텐츠 데이터의 판매 가격을 표시하는 가격표 데이터(312)는 사용자가 콘텐츠 데이터 구매 방식을 결정할 때 소정의 출력 수단을 통해 SAM(305₁)의 외부로 출력된다.

과금 처리기(587)에 의한 과금 처리는 사용 모니터(186)의 모니터링 하에서 UCP 데이터(106) 및 UCS 데이터(166)에 의해 표시되는 라이선스 협정 조건 등의 권리 콘텐츠에 근거하여 실행된다. 즉, 사용자는 권리의 허용한도내에서 콘텐츠를 구매 및 활용할 수 있다.

과금 처리를 수행함에 있어서, 과금 처리기(587)는 사용 로그 데이터(308)을 생성 또는 갱신하고, 이를 외부 메모리 관리기(811)를 통해 외부 메모리(201)에 기록한다.

사용 로그 데이터(308)와 함께 제1 실시예에서 사용된 사용 로그 데이터(108)를 사용하여 EMD 서비스 센터(302)는 안전 컨테이너(304)에 대한 라이선스 비용의 지불을 결정한다.

과금 처리기(587)는 또한 CPU(1100)의 제어 하에서 사용자가 결정된 콘텐츠의 구매 및 사용 모드를 표시하는 UCS 데이터(166)를 생성하고, 이를 작업 메모리(200)에 기록한다.

콘텐츠의 구매 방식에는 구매자의 재생 조작 및 구매자가 사용을 위해 복사하는 것에 어떤 제한도 없는 "셀 스트루(sel l through)", 콘텐츠를 재생할 때마다 지불을 해야 하는 "페이 퍼 플레이(pay per play)" 등이 있다.

UCS 데이터(166)는 사용자가 구매 방식을 결정할 때 생성되며, 이 데이터를 이용하여 콘텐츠의 사용을 통제함으로써 사용자가 권리 한도내에서 그 콘텐츠를 사용하게끔 한다. UCS 데이터(166)에는, 콘텐츠 ID, 구매 방식, 셀 쓰루 가격, 콘텐츠를 구매한 SAM의 SAM_ID, 콘텐츠를 구매한 사용자의 USER_ID 등이 들어 있다.

소정의 구매 방식이 "플레이 당 지불", "SCMS당 지불" 또는 "복제 방지 장치 없이 N 카피당 지불" 인 경우, SCM(305₁)은 USC 데이터(166)를 실시간으로 서비스 제공자(310)에게 보내고, 서비스 제공자(310)는 EMD 서비스 센터(302)에 대해 SAM(305₁)로부터 사용 로그 데이터(308)을 얻도록 지시한다.

소정의 구매 방식이 "셀 쓰루" 인 경우, USC 데이터(166)가 실시간으로 서비스 제공자(310) 및 EMD 서비스 센터(302)로 보내진다.

도 90에 도시되어 있는 바와 같이, SAM(305₁)에서는, EMD 서비스 센터 관리자(185)를 통해 EMD 서비스 센터(302)로부터 수신한 사용자 취향 필터 데이터(900)는 서비스 제공자 관리자(580)에게로 출력된다. 그 다음에, 서비스 제공자 관리자(580)에서는, 도 89에 도시된 디코딩 모듈(905)로부터 수신되고 사용자 취향 필터 데이터(900)에 근거하여 필터링된 안전 컨테이너(304)가 선택되고, 이 선택된 안전 컨테이너(304)는 다운로드 메모리 관리자(182)로 출력된다. 이렇게 함으로써 SAM(305₁)이 콘텐츠 데이터 C의 구매에 근거하여 사용자와 계약을 체결한 모든 서비스 제공자(310)으로부터 얻은 사용자의 취향에 따라 콘텐츠 데이터 C를 선택할 수 있게 된다.

SAM(305₁)내에서의 프로세스의 흐름은 이하와 같다.

라이센스 키 데이터를 수신할 때 실행되는 처리

EMD 서비스 센터(302)로부터 수신한 라이센스 키 데이터(KD₁ 내지 KD₃)를 기억부(192)에 기억시키기 위한 SAM(305₁)내에서의 프로세스의 흐름은 도 35를 참조하여 설명한 제1 실시예와 유사하다.

서비스 제공자(310)로부터 안전 컨테이너(304)를 수신할 때 실행될 처리

서비스 제공자(310)로부터 안전 컨테이너(304)를 수신할 때 SAM(305₁)내에서의 프로세스의 흐름에 대해서는 도 93을 참조하여 이하에서 기술한다.

이하의 예에서, SAM(305₁)에서는 안전 컨테이너(304)를 수신할 때 여러가지 형태의 서명 데이터를 점검한다. 그러나, 서명 데이터는 안전 컨테이너(304)를 수신할 때보다는 구매 및 사용 모드를 결정할 때 점검되어도 된다.

단계 S93-0에서, 도 90에 도시된 SAM(305₁)의 CPU(1100)는 호스트 CPU(810)로부터 안전 컨테이너를 수신하기 위한 처리를 수행하는 명령을 나타내는 내부 인터럽트(S810)를 수신한다.

단계 S93-1에서는, 도 90에 도시한 SAM(305₁)의 상호 인증부(170)가 서비스 제공자(310)과의 상호 인증을 수행한다.

그 다음에, 단계 S93-2에서, SAM(305₁)의 상호 인증부(170)는 다운로드 메모리(167)의 매체 SAM(305₁)와의 상호 인증을 수행한다.

단계 S93-3에서, 서비스 제공자(310)로부터 수신된 안전 컨테이너(304)는 다운로드 메모리(167)에 기록된다. 동시에, 안전 컨테이너(304)는 상호 인증부(170)에서 암호화되고, 단계 S93-2에서 얻은 세션 키 데이터를 사용하여 매체 SAM(167a)에서 해독된다.

단계 S93-4에서는, SAM(305₁)은 단계 S93-1에서 얻은 세션 키 데이터를 사용하여 안전 컨테이너(304)를 암호해제화한다.

뒤이어, 단계 S93-5에서, 서명 처리기(589)는 도 84D에 도시된 서명 데이터 SIG_{61,ESC}를 확인한 다음에, 도 84D에 도시된 공개-키 인증 데이터 CER_{SP}에 기억된 서비스 제공자(310)의 공개 키 데이터 K_{SP,P}를 사용하여 서명 데이터 SIG_{62,SP}, SIG_{63,SP}, 및 SIG_{64,SP}의 정당성(integrity)를 확인한다.

서명 데이터 SIG_{62,SP}의 정당성을 확인할 때, 콘텐츠 파일 CF의 발송자의 정당성을 확인한다. 서명 데이터 SIG_{63,SP}의 정당성을 확인할 때, 키 파일 KF의 발송자의 정당성을 확인한다. 서명 데이터 SIG_{64,SP}의 정당성을 확인할 때, 가격표 데이터(312)의 생성자 및 발송자의 정당성을 확인한다.

단계 S93-6에서, 서명 처리기(589)는 도 84D에 도시된 서명 데이터 SIG_{1,ESC}를 확인한 다음에, 도 84D에 도시된 공개-키 인증 데이터 CER_{CP}에 기억된 콘텐츠 제공자(301)의 공개 키 데이터 K_{CP,P}를 사용하여 서명 데이터 SIG₆, CP 및 SIG_{7,CP}를 확인한다.

서명 데이터 SIG_{6,CP}의 정당성을 확인할 때, 콘텐츠 파일 CF의 생성자 및 발송자의 정당성을 확인한다. 서명 데이터 SIG_{7,CP}의 정당성을 확인할 때, 키 파일 KF의 발송자의 정당성을 확인한다.

단계 93-7에서, 서명 처리기(589)는 기억부(192)로부터 판독한 공개 키 데이터 K_{ESC,P}를 사용하여 도 84B에 도시된 키 파일 KF내의 서명 데이터 SIG_{K1,ESC}를 점검하여 EMD 서비스 센터(302)에서 키 파일 KF의 생성자의 정당성 및 키 파일 KF의 공식 등록을 확인한다.

그 다음에, 단계 S93-8에서, 암호화/해독부(172)는 기억부(192)로부터 판독한 대응 기간의 라이선스 키 데이터 KD₁ 내지 KD₃를 사용하여 도 84B에 도시된 키 파일 KF내의 콘텐츠 키 데이터 K_C, UCP 데이터(106), 및 SAM 프로그램 다운로드 컨테이너 SDC₁ 내지 SDC₃를 해독하고, 이들을 작업 메모리(200)에 기록한다.

단계 S93-9에서, CPU(1100)는 안전 컨테이너를 수신하기 위한 상기 처리가 제대로 수행되었는지 여부를 판정하여 외부 인터럽트를 통해 호스트 CPU(810)에 해당 정보를 보고한다.

이와는 달리, CPU(1100)는 상기 처리가 적절히 수행되었는지 여부를 나타내는 SAM 상태 레지스터내의 플래그를 세트시켜도 되며, 호스트 CPU(810)는 폴링함으로써 이 플래그를 판독해도 된다.

다운로드된 안전 컨테이너의 구매 방식을 결정하기 위한 처리

다운로드된 안전 컨테이너의 구매 방식을 결정하기 위한 처리는 기본적으로 도 38을 참조하여 설명한 제1 실시예의 SAM(105₁)에 의해 수행되는 것과 유사하다. 이 처리에 따르면, 이후에 논의하게 될 도 97C에 도시된 키 파일 KF₁은 작업 메모리(200) 및 다운로드 메모리 관리자(182)를 통해 다운로드 메모리(167)에 기억된다.

콘텐츠 데이터의 재생 처리

구매 방식이 결정되고 다운로드 메모리(167)에 기억되어 있는 콘텐츠 데이터 C의 재생 처리는 기본적으로 도 40을 참조하여 설명한 제1 실시예의 SAM(105₁)에 의해 수행되는 처리와 유사하다.

한 머신의 UCS 데이터(166)이 다른 머신내의 콘텐츠를 재구매하기 위해 활용될 때 실행되는 처리

도 94에 도시된 네트워크 장치(360₁)의 다운로드 메모리(167)에 다운로드된 콘텐츠 파일 CF의 구매 방식을 결정 한 후에는, 콘텐츠 파일 CF를 기억하는 새로운 안전 컨테이너(304x)가 생성되고, 버스(191)를 통해 A/V 머신(360₂)내의 SAM(305₁)로부터 SAM(305₂)로 전송된다. 이 SAM(305₁)에서의 처리에 대해서는 도 95 및 96을 참조하여 이하에서 논의한다.

도 96의 플로우차트로 나타난 처리를 실행한다. 여기서는, 도 97C에 도시된 키 파일 KF₁ 및 그에 대한 해쉬값 H_{K1}은 상기한 구매 처리에 따라 SAM(305₁)의 작업 메모리(200)에 기억되어 있는 것으로 가정하였다.

단계 S96-1에서, 도 88 및 94에 도시된 조각부(165)에서의 사용자의 조작에 따라, 구매 방식이 결정된 안전 컨테이너를 SAM(305₂)에 전송하도록 지시하는 내부 인터럽트(S810)는 도 95에 도시된 호스트 CPU(810)로부터 CPU(1100)으로 출력된다. 과금 처리기(587)는 CPU(1100)의 통제 하에서 소정의 구매 방식에 따라 외부 메모리(201)에 기억되어 있는 사용 로그 데이터(308)를 갱신한다.

단계 S96-2에서, SAM(305₁)은 제1 실시예에서 논의한 SAM 등록 리스트를 점검하여 안전 컨테이너를 수신하는 SAM(305₂)가 정식으로 등록되었는지를 판정한다. 등록되어 있는 경우에는, SAM(305₁)은 단계 S96-3의 처리를 실행한다. SAM(305₁)은 또한 SAM(305₂)가 사용자 홈 네트워크(303)내의 SAM인지 여부도 판정한다.

그 다음에, 단계 S96-3에서, 상호 인증부(170)는 상호 인증으로 얻은 세션 키 데이터 K_{SES}를 SAM(305₂)와 공유한다.

단계 S96-4에서는, SAM 관리자(190)는 콘텐츠 파일 CF 및 도 84A에 도시한 서명 데이터 SIG_{6,CP} 및 SIG_{7,CP}를 다운로드 메모리(211)로부터 판독하여 서명 처리기(189)가 SAM(305₁)의 개인 키 데이터 K_{SAM1}을 사용하여 서명 데이터 SIG_{41,SAM1}을 생성하도록 한다.

단계 S96-5에서, SAM 관리자(190)는 도 84B에 도시된 키 파일 KF 및 서명 데이터 SIG_{7,CP} 및 SIG_{63,SP}를 다운로드 메모리(211)로부터 판독하여 서명 처리기(589)가 SAM(305₁)의 개인 키 데이터 K_{SAM1}을 사용하여 서명 데이터 SIG_{42,SAM1}을 생성하도록 한다.

그 후, 단계 S96-6에서, SAM 관리자(190)는 도 97A 내지 97E에 도시된 안전 컨테이너(304x)를 생성한다.

단계 S96-7에서, 암호화/해독부(171)는 단계 S96-3에서 얻은 세션 키 데이터 K_{SES}를 사용하여 도 97A 내지 97E에 도시된 안전 컨테이너(304x)를 암호화한다.

그 다음에, 단계 S96-8에서, SAM 관리자(190)는 안전 컨테이너(304x)를 도 94에 도시된 A/V 머신(360₂)의 SAM(305₂)에 출력한다. 이 경우, SAM(305₁, 305₂)간의 상호 인증 뿐만 아니라 IEEE-1394 직렬 버신 버스(191)의 상호 인증도 수행된다.

단계 S96-9에서, CPU(1100)는 안전 컨테이너(304x)를 전송하기 위한 상기 처리가 제대로 수행되었는지 여부를 판정하여 해당 정보를 외부 인터럽트를 통해 호스트 CPU(810)에 보고한다.

이와는 달리, CPU(1100)는 상기한 처리가 정확히 수행되었는지 여부를 나타내는 SAM 상태 레지스터내의 레지스터를 세트시켜도 되고, 호스트 CPU(810)는 폴링에 의해 플래그를 판독해도 된다.

이제, 도 98, 99 및 100을 참조하면서, SAM(305₁)로부터 입력된 도 97A 내지 97E에 도시된 안전 컨테이너(304x)를 도 94에 도시된 기록 매체(RAM, 130₄)에 기록할 때의 SAM(305₂)내에서의 프로세스의 흐름에 대해 설명한다.

도 99 및 100은 상기한 처리를 도제한 플로차트이다. 기록 매체(RAM, 130₄)는 도 14에 도시한 바와 같이 비안전 RAM 영역(134), 매체 SAM(133) 및 안전 RAM 영역(132)을 포함한다.

단계 S99-0에서, 도 98에 도시한 SAM(305₂)의 CPU(1100)는 호스트 CPU(810)로부터 기록 매체상의 구매 방식이 결정된 수신된 안전 컨테이너를 기록하라는 지시를 나타내는 내부 인터럽트(S810)를 수신한다.

그 다음에, 단계 S99-1에서, SAM(305₂)는 안전 컨테이너를 발송한 SAM(305₁)이 정식으로 등록되어 있는지 여부를 판정하기 위해 SAM 등록 리스트를 점검한다. 등록되어 있는 경우에는, SAM(305₂)는 단계 S99-2를 수행한다. SAM(305₂)는 또한 SAM(305₁)이 사용자 홈 네트워크(303)내의 SAM인지 여부도 판정한다.

단계 S99-2에서는, 단계 S96-3에 대응하는 처리로서, SAM(305₂)는 상호 인증을 수행함으로써 얻어진 세션 키 데이터 KSES를 SAM(305₁)과 공유한다.

그 다음에, 단계 S99-3에서, SAM(305₂)의 SAM 관리자(190)가 도 94에 도시한 바와 같이 네트워크 장치(360₁)의 SAM(305₁)로부터 안전 컨테이너(304x)를 수신한다.

단계 S99-4에서, 암호화/해독부(171)는 단계 S99-2에서 공유된 세션 키 데이터 K_{SES}를 사용하여 SAM 관리자(190)를 통해 수신된 안전 컨테이너(304x)를 해독한다.

계속하여, 단계 S99-5에서, 해독된 안전 컨테이너(304x)내의 콘텐츠 파일 CF에 대해 도 94에 도시한 매체 구동 SAM(260)에 의한 섹터화, 섹터 헤더 부가, 스캔블럼, ECC 인코딩, 변조 및 동기화 등의 처리를 행한 다음에, 기록 매체(RAM, 130₄)의 RAM 영역(134)에 기록한다.

단계 S99-6에서, 세션 키 데이터 K_{SES}를 가지고 해독된 안전 컨테이너(304x)내의 서명 데이터 SIG_{6,CP} SIG_{62,CP} 및 SIG_{41,SAM1}, 키 파일 KF 및 서명 데이터 SIG_{7,CP} SIG_{63,CP} 및 SIG_{42,SAM1}, 키 파일 KF₁ 및 해쉬값 H_{K1}, 공개 키 서명 데이터 CER_{SP} 및 서명 데이터 SIG_{1,ESC}, 및 공개 키 서명 데이터 CER_{SAM1} 및 서명 데이터 SIG_{22,ESC}가 작업 메모리(200)에 기록된다.

단계 S99-7에서, 서명 처리기(589)에서는, 작업 메모리(200)에서 판독한 서명 데이터 SIG_{61,ESC}, SIG_{1,ESC} 및 SIG_{22,ESC}를 기억부(192)로부터 판독한 공개 키 데이터 K_{ESC,P}를 사용, 점검하여 공개 키 인증 데이터 CER_{SP}, CER_{CP} 및 CER_{SAM1}의 정당성을 확인하게 된다.

그 다음에, 서명 처리기(589)에서는, 서명 데이터 SIG_{6,CP}의 정당성을 공개 키 인증 데이터 CER_{CP}에 기억된 공개 키 데이터 K_{CP,P}를 사용, 확인하여 콘텐츠 파일 CF의 생성자의 정당성을 확인하게 된다. 또한, 서명 처리기(589)에서, 서명 데이터 SIG_{62,SP}의 정당성은 공개 키 인증 데이터 CER_{SP}에 기억된 공개 키 데이터 K_{SP,P}를 사용, 확인하여 콘텐츠 파일 CF의 발송자의 정당성을 확인하게 된다. 서명 처리기(589)는 서명 데이터 SIG_{41,SAM1}의 정당성을 공개 키 인증 데이터 CER_{SAM1}에 기억된 공개 키 데이터 K_{SAM1,P}를 사용, 확인하여 콘텐츠 파일 CF의 발송자의 정당성을 확인하게 된다.

단계 S99-8에서, 서명 처리기(589)에서는, 서명 데이터 SIG_{7,CP}, SIG_{63,SP} 및 SIG_{42,SAM1}의 정당성은 공개 키 인증 데이터 CER_{CP}, CER_{SP}, 및 CER_{SAM1}에 각각 기억된 공개 키 데이터 K_{CP,P}, K_{SP,P} 및 K_{SAM1,P} 사용하여 확인하게 된다.

그 다음에, 단계 S99-9에서, 신호 처리기(589)에서는, 도 97B에 도시된 키 파일 KF에 기억된 서명 데이터 SIG_{K1,ESC}의 정당성을 기억부(192)로부터 판독한 공개 키 데이터 K_{ESC,P}를 사용, 확인하여 키 파일 KF의 생성자의 정당성을 확인하게 된다.

단계 S99-10에서, 서명 처리기(589)는 해쉬값 H_{K1}의 정당성을 점검하여 키 파일 KF₁의 생성자 및 발송자를 확인한다.

본 실시예에서, 키 파일 KF₁의 생성자 및 발송자는 동일하다. 그러나, 이들이 서로 다를 경우, 생성자에 대한 서명 데이터와 발송자에 대한 서명 데이터가 생성되고, 양 서명 데이터의 정당성이 신호 처리기(589)에서 확인된다.

단계 S99-11에서, 사용 모니터(186)는 단계 S99-10에서 해독된 키 파일 K_{F1}에 기억된 UCS 데이터(166)를 사용하여 콘텐츠 데이터 C의 구매 및 사용 모드를 제어하기 시작한다.

그 다음에, 단계 S99-12에서, 사용자는 조작부(165)를 조작하여 구매 방식을 판정하고, 대응하는 조작 신호(S165)가 과금 처리기(587)로 출력된다.

단계 S99-13에서, 과금 처리기(587)는 외부 메모리(201)에 기억된 사용 로그 데이터(308)를 조작 신호(S165)에 근거하여 갱신한다. 과금 처리기(587)는 또한 콘텐츠 데이터 C의 구매 모드가 판정될 때마다 판정된 구매 모드에 따라 UCS 데이터(166)도 갱신한다.

계속하여, 단계 S99-14에서, 암호화/해독부(173)는 기억 키 데이터 K_{STR} , 매체 키 데이터 K_{MED} , 기억부(192)로부터 판독한 구매자 키 데이터 K_{PIN} 를 순차 사용하여 단계 S99-12에서 발생된 UCS 데이터(166)를 암호화하고, 이 암호화된 UCS 데이터(166)를 매체 구동 SAM 관리자(855)로 출력한다.

단계 S99-15에서, 매체 드라이브 SAM 매니저(855)는, 새로운 UCS 데이터(166)를 저장하고 이를 기록 매체(RAM)(130₄)의 안전한 RAM 에리어(132)에 기록하는 키 파일 KF_1 에 대한 구역화, 섹터 헤더 추가, 스캔블럼, ECC 부호화, 변조 및 동기 등의 처리를 행한다.

그 다음, 단계 S99-16에서, 키 파일 KF_1 가 워크 메모리(200)로부터 판독된 다음, 매체 구동 SAM 매니저(855)를 통해서도 94에 도시된 매체 드라이브 SAM(260)에 의해 기록 매체(RAM)(130₄)의 안전한 RAM 에리어(132) 내로 기록된다.

단계 S99-17에서, CPU(1100)는 상술한 처리가 정확하게 행해졌는 지 여부를 결정하고, 대응하는 정보를 외부 인터럽트를 통해 호스트 CPU(810)에 보고한다.

대안적으로는, CPU(1100)는 상술한 처리를 정확하게 행하였는 지 여부를 나타내는 SAM 내에 상태 레지스터 내에 플래그를 설정할 수 있고, 호스트 CPU(810)는 포올링에 의해 플래그를 판독할 수 있다.

기록 매체(ROM)에 의해 콘텐츠 데이터의 구매 모드를 결정한 이후의, 기록 매체(ROM)에 의해 콘텐츠 데이터의 구매 모드를 결정하기 위한 처리와, 콘텐츠 데이터를 기록 매체(RAM)에 기록하기 위한 처리는, 개인 키 데이터 $K_{SP,P}$ 를 사용함으로써 서비스 제공자(310)에 의해 부가된 시그니처 데이터 SIG_{SP} 를 체크하는 것을 제외하고는 제1 실시예의 SAM(305₁)에 의해 행해지는 처리와 동일하다.

SAM(305₁)을 실행하기 위한 방법은 제1 실시예의 SAM(105₁)의 방법과 동일하다.

제1 실시예에서 설명된 사용자 홈 네트워크(103)의 구성은 사용자 홈 네트워크(303)에서 사용된 장치에 적용가능하다. 이 경우, 도 64 내지 79를 참조하여 설명된 제1 실시예의 구성은 SAM(305₁), A/V 압축/압축 해제 SAM(163), 매체 드라이브 SAM(260) 및 매체 SAM(133)의 회로 모듈에 적용할 수 있다.

유사하게, 도 62를 참조하여 설명된 보안 기능은, 콘텐츠 제공자(101)를 서비스 제공자(310)로 대신할 수 있는 것을 제외하고는 EMD 시스템(300)의 것에 적용할 수 있다.

사용자 홈 네트워크(303)에서의 여러 장치의 접속 모델은 다음과 같다.

도 101은 사용자 홈 네트워크(303)에서의 장치 모델의 접속 예를 도시한다.

도 101에 도시된 바와 같이, 네트워크 장치(360₁), A/V 머신(360₂ 및 360₃)이 IEEE-1394 직렬 버스(191)를 통해서 상호 각각 접속된다.

네트워크 장치(360₁)는 외부 메모리(201), SAM(305₁), CA 모듈(311), A/V 압축/압축 해제 SAM(163) 및 다운로드 메모리(167)를 포함한다.

CA 모듈(311)은 공중선과 같은 네트워크를 통해 서비스 제공자(310)와 통신한다. SAM(305₁)은 공중선과 같은 네트워크를 통해 EMD 서비스 센터(302)와 통신한다. 다운로드 메모리(167)로서, 매체 SAM(167a) 또는 하드 디스크 드라이브(HDD)를 구비하는 메모리 스틱을 사용할 수 있다. 다운로드 메모리(167)는 서비스 제공자(310)로부터 다운로드된 보안 용기(304)를 저장한다.

각 장치는 ATRAC3 및 MPEG과 같은 여러 압축/압축 해제 방법과 호환성이 있는 다수개 A/V 압축/압축 해제 SAM(163)을 통합한다.

SAM(305₁)은 접속형 또는 비접속형 IC 카드(1141)와 통신할 수 있다. IC 카드(1141)는 사용자 ID 등의 수개 유형의 데이터를 저장하고 SAM(305₁)에서의 사용자 확인을 행하는 데 사용된다.

A/V 머신(360₂)은 예를 들면 저장 장치이고, SAM(305₁)과 SAM(305₂) 사이에 사전설정된 처리를 행한 다음 IEE E-1394 직렬 버스(191)를 통해 네트워크 장치(360₁)로부터 수신된 보안 용기가 기록 매체(130) 상에 기록된다.

이와 유사하게, A/V 머신(360₃)은 예를 들면 저장 장치이고, SAM(305₁)과 SAM(305₂) 사이에 사전설정된 처리를 행한 다음 IEEE-1394 직렬 버스(191)를 통해 네트워크 장치(360₂)로부터 수신된 보안 용기가 기록 매체(130) 상에 기록된다.

도 101에 도시된 예에서, 매체 SAM(133)은 기록 매체(130) 상에 로드된다. 그러나, 매체 SAM(133)이 기록 매체(130)로 제공되지 않는다면, SAM(305₂)과 SAM(305₃) 사이의 상호 확인은 도 101의 1-점 쇄선 방향으로 표시된 매체 드라이브 SAM(260)을 사용함으로써 행해진다.

도 82에 도시된 EMD 시스템(300)의 전체 동작을 도 102 및 103을 참조하여 이하에서 설명하기로 한다.

이 경우, 보안 용기(304)는 예를 들면 서비스 제공자(310)로부터 온라인으로 사용자 홈 네트워크(303)로 송신된다. 콘텐츠 제공자(301), 서비스 제공자(310), 및 EMD 서비스 센터(302) 내의 SAM(305₁ 내지 305₄)의 등록이 완료된다.

도 102를 참조하면, 단계 S21에서, EMD 서비스 센터(302)에서, EMD 서비스 센터(302)의 서명 데이터 SIG_{1,ESC}와 함께 콘텐츠 제공자(301)의 공개 키 데이터 K_{CP,P}의 공개 키 인증 CER_{CP}를 콘텐츠 제공자(301)에게 송신한다.

EMD 서비스 센터(302)는 또한 서비스 제공자(310)에게, EMD 서비스 센터(302)의 서명 데이터 SIG_{1,ESC}와 함께 서비스 제공자(310)의 공개 키 데이터 K_{SP,P}의 공개 키 인증 CER_{SP}를 송신한다.

EMD 서비스 센터(302)는 또한 3개월 동안 각각이 1개월의 유효 기간을 갖는 라이선스 키 데이터 KD₁ 내지 KD₃를 사용자 홈 네트워크(303)의 SAM(305₁ 내지 305₄)으로 전송한다.

단계 S22에서, 상호 인증을 행한 다음, 콘텐츠 제공자(301)는 UCP 데이터(106)와 콘텐츠 키 데이터 K_C를 EMD 서비스 센터(302)에 등록함으로써 이들을 인증한다. EMD 서비스 센터(302)는 도 3b에 도시된 6개월 동안의 키파일 KF를 생성하고 이를 콘텐츠 제공자(301)에게 송신한다.

그러면 단계 S23에서, 콘텐츠 제공자(301)는 도 3a에 도시된 콘텐츠 파일 CF와 서명 데이터 SIG_{6,CP}와, 도 3b에 도시된 키파일 KF 및 서명 데이터 SIG_{7,CP}를 생성하고, 보안 용기(104) 내에 상술한 파일 및 서명 데이터와, 공개 키 인증 데이터 CER_{CP} 및 서명 데이터 SIG_{1,ESC}는 온 라인 및/또는 오프 라인을 통해 서비스 제공자(310)에 저장된다.

단계 S24에서, 도 3c에 도시된 서명 데이터 SIG_{1,ESC}를 조사한 다음, 서비스 제공자(310)는 공개 키 인증 데이터 CER_{CP}에 저장된 공개 키 데이터 K_{CP,P}를 사용함으로써 도 3a 및 3b에 도시된 서명 데이터 SIG_{6,CP}와 SIG_{7,CP}의 완전성(integrity)을 확인함으로써, 보안 용기(104)가 법정 콘텐츠 제공자(301)로부터 전송되었음을 확인한다.

이어서, 단계 S25에서, 서비스 제공자(310)는, 가격 태그 데이터(312)와 서명 데이터 SIG_{64,SP}를 생성함으로써 도 87에 도시된 보안 용기(304)에 상술한 데이터가 저장되도록 한다.

단계 S26에서, 서비스 제공자(310)는 EMD 서비스 센터(302)에 가격 태그 데이터를 등록함으로써 이를 인증한다.

단계 S27에서, 서비스 제공자(310)는 단계 S25에서 생성된 보안 용기(304)를 예를 들면, 사용자 홈 네트워크(303)의 CA 모듈(311)로부터의 요청에 응답하여 온 라인 또는 오프 라인으로도 89에 도시된 네트워크 장치(360₁)의 디코딩 모듈(905)로 전송한다.

그런 다음, 단계 S28에서, CA 모듈(311)은 SP 구매 로그 데이터(309)를 생성하여 이를 서비스 제공자(310)에게로 적절히 전송한다.

도 103을 참조하면, 단계 S29에서, 도 84d에 도시된 서명 데이터 SIG_{61,ESC}의 완전성을 검증한 다음, SAM(305₁ 내지 305₄) 중 하나가 공개 키 인증 데이터 CER_{SP}에 저장된 공개 키 데이터 K_{SP,P}를 사용함으로써, 도 84a, 84b 및 84c에서 도시된 서명 데이터 SIG_{62,SP}, SIG_{63,SP}, SIG_{64,SP}의 완전성을 검증함으로써, 보안 용기(304) 내의 사전 설정된 데이터가 생성되었는 지 여부 및 법적 서비스 제공자(310)에게로 전송되었는 지 여부를 결정한다.

그런 다음, 단계 S30에서, 도 84d에 도시된 서명 데이터 SIG_{1,ESC}의 완전성을 검증한 다음, SAM(305₁ 내지 305₄) 중 하나가 공개 키 인증 데이터 CER_{CP}에 저장된 공개 키 데이터 K_{CP,P}를 사용함으로써, 보안 용기(304) 내의 콘텐츠 파일 CF가 법적 콘텐츠 제공자(310)에게로 전송되었는 지 여부, 및 키 파일 KF가 법적 콘텐츠 제공자(301)에게로 전송되었는 지 여부를 결정한다.

또한, SAM(305₁ 내지 305₄) 중 하나가 공개 키 인증 데이터 K_{ESC,P}를 사용함으로써 도 84b에 도시된 키 파일 KF 내의 서명 데이터 SIGK_{1,ESC}의 완전성을 검증함으로써, 키 파일 KF가 법적 ESD 서비스 센터(302)에 의해 생성되었는 지 여부를 결정한다.

단계 S31에서, 사용자는 도 88에 도시된 동작부(165)를 동작시킴으로써 콘텐츠의 구매 및 사용 모드를 결정한다.

단계 S32에서, SAM(305₁ 내지 305₄)을 통하여, 보안 용기(304)의 사용 로그 데이터(308)가 호스트 CPU(810)로부터 단계 S31의 SAM(305₁ 내지 305₄)으로 출력된 내부 인터럽트 S810에 기초하여 생성된다.

사용 로그 데이터(308)와 서명 데이터 SIG_{205,SAMI}가 SAM(305₁ 내지 305₄)으로부터 EMD 서비스 센터(302)로 전송된다. USC 데이터(166)는 구매 모드가 결정되는 실시간마다 SAM(305₁ 내지 305₄)으로부터 EMD 서비스 센터(302)로 전송된다.

단계 S33에서, EMD 서비스 센터(302)는 사용자 로그 데이터(308)에 기초하여 콘텐츠 제공자(301)와 서비스 제공자(310) 각각의 과금 콘텐츠(accounting content)를 결정(계산)하고, 이 과금 콘텐츠에 기초하여 조정 요청 데이터(152c)를 생성한다.

이어서, 단계 S34에서, EMD 서비스 센터(302)는 EMD 서비스 센터(302)의 서명 데이터와 함께 조정 요청 데이터(152c 및 152s)를 지불 통로(90)를 통하여 조정 기구(91)로 전송한다. 따라서, 사용자 홈 네트워크(303)의 사용자에 의해 이루어진 지불은 콘텐츠 제공자(301), 콘텐츠 권리 홀더, 서비스 제공자(310) 및 서비스 제공자 권리 홀더에게로 분배된다.

상술한 바와 같이, EMD 시스템(300)에서, 도 3a 내지 3c에 도시된 보안 용기(104)는 콘텐츠 제공자(301)로부터 서비스 제공자(310)로 할당되고, 보안 용기(304) 내에 있는 콘텐츠 파일 CF와 보안 용기(104)의 키 파일 KF는 서비스 제공자(310)로부터 사용자 홈 네트워크(303)로 전송된다. 키 파일 KF에 대한 처리는 SAM(305₁ 내지 305₄)에서 실행된다.

키 파일 KF에 저장된 콘텐츠 키 데이터 Kc와 UCP 데이터(106)은 라이선스 키 데이터(KD₁ 내지 KD₃)로 암호화되고 상기 라이선스 키 데이터(KD₁ 내지 KD₃)를 홀딩하는 SAM(305₁ 내지 305₄)에서만 암호해독된다. SAM(305₁ 내지 305₄)은 변경-저항 모듈로서, UCP 데이터(106)에 기술된 콘텐츠 데이터 C의 취급 증서에 기초하여 콘텐츠 데이터 C의 구매 및 사용 모드를 결정한다.

결과적으로, EMD 시스템(300)에 따르면, 사용자 홈 네트워크(303)의 콘텐츠 데이터 C는 서비스 제공자(310)의 처리와는 관계없이, 콘텐츠 제공자(301) 또는 콘텐츠-제공자와 관련된 구조에 의해 생성된 UCP 데이터(106)에 기초하여 확실하게 구매되어 사용될 수 있다. 즉, EMD 시스템(300)에서, UCP 데이터(106)는 서비스 제공자(310)에 의해 관리될 수 없다.

그리하여 EMD 시스템(300)에서, 콘텐츠 데이터 C가 다수의 다른 서비스 제공자(310)를 통해 사용자 홈 네트워크(303)로 분산되고, 사용자 홈 네트워크(303)의 SAM에서 콘텐츠 데이터 C에 대한 권리 처리는 콘텐츠 제공자(301) 또는 콘텐츠 제공자와 관련된 구조에 의해 생성된 공통 UCP 데이터(106)에 기초하여 행해질 수 있다.

EMD 시스템(300)에서, 보안 용기(104 및 304) 내의 파일 및 데이터가 서명 데이터로 제공되고, 여기서 파일 및 데이터의 생성자 및 전송자를 검증한다. 그리하여, 서비스 제공자(310)와 SAM(305₁ 내지 305₄)로 하여금 파일 및 데이터의 완전성, 파일 및 데이터의 생성자 및 전송자의 완전성을 체크함으로써 콘텐츠 데이터 C의 불법적 사용을 효율적으로 방지할 수 있다.

EMD 시스템(300)에서, 보안 용기(304)는 온 라인 또는 오프 라인으로 전송되는 지 여부에 상관없이, 서비스 제공자(310)로부터 사용자 홈 네트워크(303)로 콘텐츠 데이터 C를 분배하기 위해 사용된다. 사용자 홈 네트워크(303)의 SAM(305₁ 내지 305₄)으로 하여금 보안 용기(304)를 온 라인 또는 오프 라인으로 송신하는 지 여부에 상관없이 동일한 권리 처리를 행할 수 있게 한다.

사용자 홈 네트워크(303) 내에서 네트워크 장치(360₁) 및 A/V 머신(360₂ 내지 360₄)의 콘텐츠 데이터 C의 구매, 사용, 기록 및 이송 중에서, UCP 데이터(106)에 기초하여 처리가 실행된다. 그리하여, 전체 사용자 홈 네트워크(303)에 공통으로 권리 처리 룰을 설치할 수 있다.

예를 들면 도 104에 도시된 바와 같이, 콘텐츠 제공자(301)로부터 제공된 콘텐츠 데이터 C는 서비스 제공자(310)로부터 패킷지 분산, 디지털 방송, 인터넷, 전송선, 디지털 라디오, 또는 이동 통신 등의 어떤 방법(경로)에 의해 사용자 홈 네트워크(303)에 분산될 수 있다. 상술한 방법 중 어떤 하나를 사용한다 하더라도, 공통의 권리 처리 룰을 콘텐츠 제공자(301)에 의해 생성된 UCP 데이터(106)에 기초하여 사용자 홈 네트워크(303 및 303a)의 SAM에서 사용할 수 있다.

EMD 시스템(300)에 따르면, EMD 서비스 센터(302)는 인증 기능, 키-데이터 관리 기능, 및 권리 처리(분산 금지) 기능을 갖는다. 그리하여, 사용자에 의해 이루어진 지불은 사전설정된 비율에 따라 콘텐츠 제공자(301) 및 EMD 서비스 센터(302)로 확실하게 분산될 수 있다.

또한, 동일한 콘텐츠 제공자(301)로부터 제공된 동일한 콘텐츠 파일 CF의 UCP 데이터(106)가 서비스 제공자(310)의 서비스와는 상관없이 SAM(305₁ 내지 305₄)으로 제공된다. 따라서, 콘텐츠 파일 CF를 콘텐츠 제공자(301)의 판단으로 UCP 데이터(106)에 기초하여 SAM(305₁ 내지 305₄)에서 사용할 수 있다.

즉, EMD 시스템(300)에 따르면, 콘텐츠 서비스의 제공 또는 사용자가 콘텐츠를 사용하는 데 있어, 통상적으로 요구된 가사 기관(725)에 의지하지 않고도 기술 수단에 따라 콘텐츠 제공자(301)의 권리와 이익을 확실히 보호할 수 있다.

예를 들면, 제2 실시예의 EMD 시스템(300)에서 사용된 보안 용기에 대한 분산 프로토콜을 다음에서와 같이 설명한다.

콘텐츠 제공자(301)에서 생성된 보안 용기(104)는 도 105에 도시된 바와 같이, 인터넷(TCP/IP) 또는 전용선(ATM 셀)과 같은 콘텐츠 제공자 분산 프로토콜을 사용함으로써 서비스 제공자(301)에게로 분산된다.

서비스 제공자(310)는 보안 용기(104)로부터 사용자 홈 네트워크(303)로 생성된 보안 용기(104)를, 디지털 방송(MPEG-TS에서의 XML/SMIL) 인터넷(TCP/IP에서의 XML/SMIL) 또는 패킷지 분산(기록 매체) 등의 서비스-제공자 분산 프로토콜을 사용함으로써 분산시킨다.

사용자 홈 네트워크(303 또는 303a) 내에서 또는 사용자 홈 네트워크(303 및 303a) 사이에서 또는 SAMs 사이에서, 보안 용기는 홈 전기 상용품(EC)/분산 서비스(1394) 적렬 버스 인터페이스에서의 XML/SMIL) 또는 기록 매체를 사용함으로써 이동된다.

본 발명에서 현재 고려하고 있는 바람직한 실시예를 참조하여 설명하였더라도, 본 발명이 나타난 실시예들에만 제한되는 것은 아님을 주지하기 바란다.

예를 들면, 전술한 실시예들에서는 키 파일 KF가 EMD 서비스 센터 (102 또는 302)에서 생성되었다 하더라도, 콘텐츠 제공자(101 또는 301)에서도 생성될 수 있다.

발명의 효과

전술한 설명에서 볼 때, 본 발명의 데이터 처리 장치는 다음과 같은 장점을 제공한다. 콘텐츠 데이터의 권리 처리는 보안 환경에서 콘텐츠 데이터의 취급을 나타내는 UCP 데이터에 기초하여 실행될 수 있다. 그 결과, UCP 데이터가 콘텐츠 제공자에 의해 생성된다면, 콘텐츠 데이터의 이익이 적절하게 보호될 수 있고 또한, 콘텐츠 제공자에 의해 모니터링된 부하도 감소될 수 있다.

(57) 청구의 범위

청구항 1.

사용 제한 정책 데이터에 근거하여 콘텐츠 키 데이터로 암호화된 콘텐츠 데이터의 정상 처리를 실시하고, 암호화된 콘텐츠 키 데이터를 해독하기 위한 데이터 처리 장치에 있어서,

제1 버스;

상기 제1 버스에 접속되고, 상기 사용 제한 정책 데이터에 근거하여 상기 콘텐츠 데이터의 정상 처리를 실시하는 연산 처리 회로;

상기 제1 버스에 접속된 기억 회로;

제2 버스;

상기 제1 버스와 상기 제2 버스 사이에 배치된 제1 인터페이스 회로;

상기 제2 버스에 접속되어 상기 콘텐츠를 키 데이터를 해독하는 암호 처리 회로; 및

상기 제2 버스에 접속된 외부 버스 인터페이스 회로

를 조작 방지 회로 (tamper-resistant circuit) 모듈내에 포함하는 것을 특징으로 하는 데이터 처리 장치.

청구항 2.

제1항에 있어서, 상기 조작 방지 회로 모듈내에 제2 인터페이스 회로를 더 포함하고, 상기 제1 버스는 상기 연산 처리 회로와 상기 기억 회로에 접속된 제3 버스 및 상기 제1 인터페이스 회로에 접속된 제4 버스를 포함하며, 상기 제2 인터페이스 회로는 상기 제3 버스 및 상기 제4 버스 사이에 배치되는 것을 특징으로 하는 데이터 처리 장치.

청구항 3.

제2항에 있어서, 상기 조작 방지 회로 모듈내에

제5 버스;

상기 제5 버스에 접속되어, 기록 매체와 접촉회로 카드중 하나에 로드되는 인증 기능을 갖춘 데이터 처리 회로와의 통신을 실시하는 제3 인터페이스 회로; 및

상기 제4 버스와 상기 제5 버스 사이에 배치된 제4 인터페이스 회로

를 더 포함하는 것을 특징으로 하는 데이터 처리 장치.

청구항 4.

제1항에 있어서, 상기 암호 처리 회로는 공개 키 (public - key) 암호 회로 및 공통 키 (common - key) 암호 회로를 포함하는 것을 특징으로 하는 데이터 처리 장치.

청구항 5.

제4항에 있어서, 상기 기억 회로는 상기 데이터 처리 장치의 전용 키 (private key) 데이터 및 제2 데이터 처리 장치의 공개 키 데이터를 기억하고;

상기 공개 키 암호 회로는 상기 콘텐츠 데이터, 상기 콘텐츠 키 데이터, 상기 사용 제한 정책 데이터의 완전성 (integrity)을 검증하는 서명 데이터의 완전성을 대응하는 공개 키 데이터를 사용하여 검증하며, 상기 콘텐츠 데이터, 상기 콘텐츠 키 데이터, 상기 사용 제한 정책 데이터를 기록 매체에 기록하거나 이들을 상기 제2 데이터 처리 장치로 전송할 때에, 상기 공개 키 암호 회로는 상기 콘텐츠 데이터, 상기 콘텐츠 키 데이터, 상기 사용 제한 정책 데이터의 완전성을 검증하는 서명 데이터를 상기 전용 키 데이터를 사용하여 생성하며;

상기 공통 키 암호 회로는 상기 콘텐츠 키 데이터를 해독하고, 상기 콘텐츠 데이터, 상기 콘텐츠 키 데이터, 상기 사용 제한 정책 데이터를 온라인으로 상기 제2 데이터 처리 장치로 전송할 때에, 상기 공통 키 암호 회로는 상기 제2 데이터 처리 장치와의 상호 인증을 실시하여 구해진 세션 키 데이터를 사용하여 상기 콘텐츠 데이터, 상기 콘텐츠 키 데이터, 상기 사용 제한 정책 데이터를 암호화하고 해독하는 것을 특징으로 하는 데이터 처리 장치.

청구항 6.

제5항에 있어서, 상기 조작 방지 회로 모듈내에 상기 콘텐츠 데이터, 상기 콘텐츠 키 데이터, 상기 사용 제한 정책 데이터의 해쉬값을 발생시키기 위한 해쉬값 발생 회로를 더 포함하고, 상기 공개 키 암호 회로는 상기 해쉬값을 이용하여 상기 서명 데이터의 완전성을 검증하고 서명 데이터를 생성하는 것을 특징으로 하는 데이터 처리 장치.

청구항 7.

제1항에 있어서, 상기 조작 방지 회로 모듈내에 난수 발생 회로를 더 포함하고, 상기 난수 발생 회로는 상기 제2 버스에 접속되어, 상기 콘텐츠 데이터, 상기 콘텐츠 키 데이터, 상기 사용 제한 정책 데이터를 온라인으로 상기 제2 데이터 처리 장치로 전송할 때에 상기 제2 데이터 처리 장치와의 상호 인증을 실시하기 위한 난수를 발생하는 것을 특징으로 하는 데이터 처리 장치.

청구항 8.

제1항에 있어서, 상기 외부 버스 인터페이스 회로는 상기 콘텐츠 데이터, 상기 콘텐츠 키 데이터, 상기 사용 제한 정책 데이터중 적어도 하나를 기억하는 외부 기억 회로에 접속된 것을 특징으로 하는 데이터 처리 장치.

청구항 9.

제8항에 있어서, 상기 연산 처리 회로로부터의 커맨드에 따라 상기 기억 회로로의 액세스 및 상기 외부 버스 인터페이스 회로를 경유한 상기 외부 기억 회로로의 액세스를 제어하기 위한 기억 회로 제어 회로를 더 포함하는 것을 특징으로 하는 데이터 처리 장치.

청구항 10.

제1항에 있어서, 상기 외부 버스 인터페이스 회로는 상기 데이터 처리 장치가 로드되는 시스템을 중앙 제어하기 위한 호스트 연산 처리 장치에 접속되는 것을 특징으로 하는 데이터 처리 장치.

청구항 11.

제8항에 있어서, 상기 기억 회로의 어드레스 공간 및 상기 외부 기억 회로의 어드레스 공간을 관리하기 위한 기억부 관리 회로를 더 포함하는 것을 특징으로 하는 데이터 처리 장치.

청구항 12.

제1항에 있어서, 상기 연산 처리 회로는 상기 사용 제한 정책 데이터에 의해 표시되는 처리 정책에 근거하여 콘텐츠 데이터의 구입 모드 및 사용 모드중 적어도 하나를 판정하고, 판정된 모드의 결과를 표시하는 로그 데이터를 생성하는 것을 특징으로 하는 데이터 처리 장치.

청구항 13.

제12항에 있어서, 구입 모드 판정 후에, 상기 연산 처리 회로는 판정된 구입 모드에 따라 사용 제한 상태 데이터를 생성하고, 상기 사용 제한 상태 데이터에 근거하여 콘텐츠 데이터의 사용을 제한하는 것을 특징으로 하는 데이터 처리 장치.

청구항 14.

제4항에 있어서, 구입 모드로 판정된 콘텐츠 데이터를 기록 매체에 기록할 때에, 상기 공통 키 암호 회로는 상기 기록 매체에 대응하는 매체 키 데이터를 사용하여 상기 콘텐츠 키 데이터 및 상기 사용 제한 상태 데이터를 암호화하는 것을 특징으로 하는 데이터 처리 장치.

청구항 15.

제4항에 있어서, 상기 콘텐츠 키 데이터가 유효 기간을 가진 라이선스 키 데이터로 암호화될 때, 상기 기억 회로는 상기 라이선스 키 데이터를 기억하고, 상기 데이터 처리 장치는 실시간을 발생하기 위한 실시간 클럭을 더 포함하며, 상기 연산 처리 회로는 상기 실시간 클럭에 의해 표시된 실시간에 근거하여 상기 기억 회로로부터 유효 라이선스 키 데이터를 판독하고, 상기 공통 키 암호 회로는 판독된 라이선스 키 데이터를 사용하여 콘텐츠 키 데이터를 해독하는 것을 특징으로 하는 데이터 처리 장치.

청구항 16.

제1항에 있어서, 상기 기억 회로는 블록 단위로 데이터를 기입 및 소거하며, 상기 데이터 처리 장치는 상기 연산 처리 회로의 제어하에 데이터를 상기 기억 회로에 블록 단위로 기입 및 소거하는 것을 제어하기 위한 기입 - 록 제어 회로를 상기 조작 방지 회로 모듈내에 포함하는 것을 특징으로 하는 데이터 처리 장치.

청구항 17.

사용 제한 정책 데이터에 근거하여 콘텐츠 키 데이터로 암호화된 콘텐츠 데이터의 정상 처리를 실시하고, 암호화된 콘텐츠 키 데이터를 해독하기 위한 데이터 처리 장치에 있어서,

제1 버스;

상기 제1 버스에 접속되고, 상기 사용 제한 정책 데이터에 근거하여 상기 콘텐츠 데이터의 정상 처리를 실시하는 연산 처리 회로;

상기 제1 버스에 접속된 기억 회로;

제2 버스;

상기 제1 버스와 상기 제2 버스 사이에 배치된 인터페이스 회로;

상기 제2 버스에 접속되어 상기 콘텐츠 키 데이터를 해독하는 암호 처리 회로; 및

상기 제2 버스에 접속된 외부 버스 인터페이스 회로

를 조작 방지 회로 모듈내에 포함하며,

상기 외부 버스 인터페이스 회로를 거쳐 외부 회로로부터 인터럽트를 수신하면, 상기 연산 처리 회로는 상기 인터럽트에 의해 지정된 처리를 실시하도록 상기 외부 회로에 대한 슬레이브가 되어, 그 연산의 결과를 상기 외부 회로에 보고하는 것을 특징으로 하는 데이터 처리 장치.

청구항 18.

제17항에 있어서, 상기 연산 처리 회로는 상기 외부 회로로 인터럽트를 출력함으로써 처리의 결과를 보고하는 것을 특징으로 하는 데이터 처리 장치.

청구항 19.

제17항에 있어서, 상기 외부 버스 인터페이스는 상기 연산 처리 회로 및 상기 외부 회로를 위한 공통 메모리를 포함하고, 상기 연산 처리 회로는 처리의 결과를 상기 공통 메모리에 기입하며, 상기 외부 회로는 풀링을 통해 처리의 결과를 구하는 것을 특징으로 하는 데이터 처리 장치.

청구항 20.

제19항에 있어서, 상기 외부 버스 인터페이스는

상기 연산 처리 회로에 상기 외부 회로로부터 요청된 처리의 실행 상태를 표시하고, 상기 연산 처리 회로에 의해 설정되며 상기 외부 회로에 의해 판독되는 플래그를 포함하는 제1 상태 레지스터;

상기 외부 회로가 상기 연산 처리 회로에 처리를 실시하도록 요청하였는지 여부를 표시하고, 상기 외부 회로에 의해 설정되며 상기 연산 처리 회로에 의해 판독되는 플래그를 포함하는 제2 상태 레지스터; 및

처리의 결과를 기억하기 위한 상기 공통 메모리

를 포함하는 것을 특징으로 하는 데이터 처리 장치.

청구항 21.

제18항에 있어서, 상기 기억 회로는 인터럽트에 의해 지정된 처리를 기술한 인터럽트 프로그램을 기억하고, 상기 연산 처리 회로는 상기 기억 회로로부터 판독된 인터럽트 프로그램을 실행하여 처리를 실시하는 것을 특징으로 하는 데이터 처리 장치.

청구항 22.

제21항에 있어서, 상기 기억 회로는 복수의 상기 인터럽트 프로그램과, 인터럽트 프로그램을 실행할 때 판독될 복수의 서브-루틴을 기억하고, 상기 연산 처리 회로는 상기 기억 회로로부터 판독된 인터럽트 프로그램을 실행할 때 상기 기억 회로로부터 서브-루틴을 적절히 판독하고 실행하는 것을 특징으로 하는 데이터 처리 장치.

청구항 23.

데이터 처리 시스템에 있어서,

선정된 프로그램을 실행하고, 마스터로서 작용하여 선정된 조건에 따라 인터럽트를 출력하는 연산 처리 장치와;

상기 연산 처리 장치에 대한 슬레이브로서 작용하여 상기 연산 처리 장치로부터의 인터럽트에 응답하여 선정된 처리를 실시하고, 처리의 결과를 상기 연산 처리 장치에 보고하는 데이터 처리 장치를 포함하며,

상기 데이터 처리 장치는

사용 제한 정책 데이터에 의해 표시되는 처리 정책에 근거하여 콘텐츠 데이터의 구입 모드 및 사용 모드중 적어도 하나를 판정하는 판정 수단;

판정된 모드의 결과를 표시하는 로그 데이터를 발생시키는 로그 데이터 발생 수단; 및

콘텐츠 키 데이터를 해독하는 해독 수단

을 조작 방식 회로 모듈내에 포함하는 것을 특징으로 하는 데이터 처리 시스템.

청구항 24.

제23항에 있어서, 인터럽트 타입을 표시하는 인터럽트를 수신하면, 상기 연산 처리 장치는 인터럽트 타입에 대응하는 인터럽트 루틴을 실행하라는 명령을 표시하는 인터럽트를 상기 데이터 처리 장치에 출력하고, 상기 데이터 처리 장치는 상기 연산 처리 장치로부터 수신된 인터럽트의 인터럽트 타입에 대응하는 인터럽트 루틴을 실행하는 것을 특징으로 하는 데이터 처리 시스템.

청구항 25.

제23항에 있어서, 상기 데이터 처리 장치는 상기 연산 처리 장치로 인터럽트를 출력함으로써 처리의 결과를 보고하는 것을 특징으로 하는 데이터 처리 시스템.

청구항 26.

제23항에 있어서, 상기 데이터 처리 장치는 상기 데이터 처리 장치 및 상기 연산 처리 장치에 의해 액세스 가능한 공통 메모리를 포함하고, 상기 연산 처리 장치는 폴링을 통해 상기 공통 메모리에 액세스함으로써 처리의 결과를 구하는 것을 특징으로 하는 데이터 처리 시스템.

청구항 27.

제26항에 있어서, 상기 데이터 처리 장치는

상기 연산 처리 장치로부터 요청된 처리의 실행 상태를 표시하고, 상기 연산 처리 장치에 의해 판독되는 플래그를 포함하는 제1 상태 레지스터;

상기 연산 처리 장치가 상기 데이터 처리 장치에 인터럽트에 의한 처리를 실시하도록 요청하였는지 여부를 표시하고, 상기 연산 처리 장치에 의해 설정되는 플래그를 포함하는 제2 상태 레지스터; 및

처리의 결과를 기억하기 위한 상기 공통 메모리

를 포함하는 것을 특징으로 하는 데이터 처리 시스템.

청구항 28.

제23항에 있어서, 상기 연산 처리 장치와 상기 데이터 처리 장치를 접속하기 위한 버스를 더 포함하는 것을 특징으로 하는 데이터 처리 시스템.

청구항 29.

제24항에 있어서, 상기 데이터 처리 장치는 초기 프로그램 및 인터럽트 루틴중 하나의 실행을 완료한 후에 저전력 상태로 들어가는 것을 특징으로 하는 데이터 처리 시스템.

청구항 30.

제24항에 있어서, 상기 연산 처리 장치로부터 수신된 인터럽트에 근거하여, 상기 데이터 처리 장치는 콘텐츠 데이터의 구입 모드 및 사용 모드중 하나를 판정하는 처리와, 콘텐츠 데이터를 재생하는 처리와, 인증 기관(certifying authority)으로부터 데이터를 다운로드하는 처리중 적어도 하나에 따라 인터럽트 루틴을 실행하는 것을 특징으로 하는 데이터 처리 시스템.

청구항 31.

제23항에 있어서, 상기 연산 처리 장치는 선정된 사용자 프로그램을 실행하는 것을 특징으로 하는 데이터 처리 시스템.

청구항 32.

데이터 처리 장치에 의해 제공되는 콘텐츠 데이터가 데이터 분배 장치로부터 수신되고 관리 장치에 의해 관리되는 데이터 처리 시스템에 있어서,

콘텐츠 키 데이터로 암호화된 콘텐츠 데이터와, 암호화된 콘텐츠 키 데이터와, 콘텐츠 데이터의 처리 정책을 표시하는 사용 제한 정책 데이터와, 상기 데이터 분배 장치에 의해 결정된 콘텐츠 데이터에 대한 가격 데이터가 기억되어 있는 모듈을 상기 데이터 분배 장치로부터 수신하고, 상기 수신된 모듈을 공통 키 데이터를 사용하여 해독하며, 상기 데이터 분배 장치에 의한 모듈의 분배 서비스에 대한 어카운팅 처리를 실시하는 제1 처리 모듈;

선정된 프로그램을 실행하고, 마스터로서 작용하여 선정된 조건에 따라 인터럽트를 출력하는 연산 처리 장치; 및

상기 연산 처리 장치에 대한 슬레이브로서 작용하여 상기 연산 처리 장치로부터의 인터럽트에 응답하여 선정된 처리를 실시하고, 처리의 결과를 상기 연산 처리 장치에 보고하는 데이터 처리 장치를 포함하며,

상기 데이터 처리 장치는

수신된 모듈에 기억되어 있는 사용 제한 정책 데이터에 의해 표시되는 처리 정책에 근거하여 콘텐츠 데이터의 구입 모드 및 사용 모드중 적어도 하나를 판정하는 판정 수단;

판정된 모드의 결과를 표시하는 로그 데이터를 발생시키는 로그 데이터 발생 수단;

콘텐츠 데이터의 구입 모드가 판정될 때 상기 관리 장치로 상기 가격 데이터 및 로그 데이터를 출력하는 출력 수단; 및

콘텐츠 키 데이터를 해독하는 해독 수단

을 조작 방지 회로 모듈내에 포함하는 것을 특징으로 하는 데이터 처리 시스템.

청구항 33.

데이터 처리 시스템에 있어서,

선정된 프로그램을 실행하고, 마스터로서 작용하여 선정된 조건에 따라 인터럽트를 출력하는 연산 처리 장치;

상기 연산 처리 장치에 대한 슬레이브로서 작용하여 상기 연산 처리 장치로부터의 인터럽트에 응답하여 콘텐츠 키 데이터로 암호화된 콘텐츠 데이터의 정상 처리를 실시하고, 처리의 결과를 상기 연산 처리 장치에 보고하는 제1 조작 방지 데이터 처리 장치; 및

상기 제1 조작 방지 데이터 처리 장치와의 상호 인증을 실시하여 구해진 콘텐츠 키 데이터를 사용하여 콘텐츠 데이터를 해독하고, 상기 연산 처리 장치 또는 상기 제1 조작 방지 데이터 처리 장치에 대한 슬레이브로서 작용하여 상기 연산 처리 장치 또는 상기 제1 조작 방지 데이터 처리 장치로부터의 인터럽트에 응답하여 콘텐츠 데이터를 압축 또는 압축해제하는 제2 조작 방지 데이터 처리 장치

를 포함하는 것을 특징으로 하는 데이터 처리 시스템.

청구항 34.

제33항에 있어서, 상기 연산 처리 장치와, 상기 제1 조작 방지 데이터 처리 장치와, 상기 제2 조작 방지 데이터 처리 장치를 접속하기 위한 버스를 더 포함하는 것을 특징으로 하는 데이터 처리 시스템.

청구항 35.

데이터 처리 시스템에 있어서,

선정된 프로그램을 실행하고, 마스터로서 작용하여 선정된 조건에 따라 인터럽트를 출력하는 연산 처리 장치;

상기 연산 처리 장치에 대한 슬레이브로서 작용하여 상기 연산 처리 장치로부터의 인터럽트에 응답하여 콘텐츠 키 데이터로 암호화된 콘텐츠 데이터의 정상 처리를 실시하고, 처리의 결과를 상기 연산 처리 장치에 보고하는 제1 조작 방지 데이터 처리 장치; 및

상기 연산 처리 장치와의 상호 인증을 실시하고, 상기 연산 처리 장치로부터의 인터럽트 출력에 응답하여 콘텐츠 데이터를 기록 매체로부터 판독하고 기록 매체에 기입하는 제2 조작 방지 데이터 처리 장치

를 포함하는 것을 특징으로 하는 데이터 처리 시스템.

청구항 36.

제35항에 있어서, 상기 제2 조작 방지 처리 장치는 상기 기록 매체에 대응하는 매체 키 데이터를 사용하여 콘텐츠 데이터를 해독 및 암호화하는 것을 특징으로 하는 데이터 처리 시스템.

청구항 37.

제35항에 있어서, 상기 기록 매체에 상호 인증 기능을 갖는 처리 회로가 제공되는 경우, 상기 제2 조작 방지 처리 장치는 상기 처리 회로와의 상호 인증을 실시하는 것을 특징으로 하는 데이터 처리 시스템.

청구항 38.

테이타 처리 시스템에 있어서,

선정된 프로그램을 실행하고, 마스터로서 작용하여 선정된 조건에 따라 인터럽트를 출력하는 연산 처리 장치;

상기 연산 처리 장치와의 상호 인증을 실시하고, 상기 연산 처리 장치로부터의 인터럽트 출력에 응답하여 콘텐츠 데이터를 기록 매체로부터 판독하고 기록 매체에 기입하는 제1 조작 방지 테이타 처리 장치; 및

콘텐츠 키 테이타를 사용하여 콘텐츠 테이타를 해독하고, 상기 연산 처리 장치에 대한 슬레이브로서 작용하여 상기 연산 처리 장치로부터의 인터럽트에 응답하여 콘텐츠 테이타를 압축 또는 압축해제하는 제2 조작 방지 테이타 처리 장치를 포함하는 것을 특징으로 하는 테이타 처리 시스템.

청구항 39.

제38항에 있어서, 상기 제1 조작 방지 테이타 처리 장치에 의해 상기 기록 매체로부터 판독된 콘텐츠 테이타를 일시적으로 기억하고, 기억된 콘텐츠 테이타를 상기 제2 조작 방지 테이타 처리 장치로 출력하는 기억 회로를 더 포함하는 것을 특징으로 하는 테이타 처리 시스템.

청구항 40.

제39항에 있어서, 상기 기억 회로는 진동 방지 기억 회로의 기억 영역 부분을 이용하는 것을 특징으로 하는 테이타 처리 시스템.

청구항 41.

제38항에 있어서, 상기 연산 처리 장치에 대한 슬레이브로서 작용하여 상기 연산 처리 장치로부터의 인터럽트에 응답하여 콘텐츠 키 테이타로 암호화된 콘텐츠 테이타의 정상 처리를 실시하고, 처리의 결과를 상기 연산 처리 장치에 보고하는 제3 조작 방지 테이타 처리 장치를 더 포함하는 것을 특징으로 하는 테이타 처리 시스템.

청구항 42.

연산 처리 장치와 테이타 처리 장치를 사용하여 테이타를 처리하는 방법에 있어서,

상기 연산 처리 장치에서, 선정된 프로그램을 실행하고, 마스터로서 작용하여 선정된 조건에 따라 인터럽트를 출력하는 단계; 및

상기 테이타 처리 장치에서, 상기 연산 처리 장치에 대한 슬레이브로서 작용하여 상기 연산 처리 장치로부터의 인터럽트에 응답하여, 조작 방지 회로 모듈내에서, 사용 제한 정책 테이타의 처리 정책에 근거하여 콘텐츠 테이타의 구입 모드 및 사용 모드중 적어도 하나를 판정하고, 판정된 모드의 결과를 표시하는 로그 테이타를 생성하며, 콘텐츠 키 테이타를 해독하는 단계

를 포함하는 것을 특징으로 하는 테이타 처리 방법.

청구항 43.

제42항에 있어서, 인터럽트 타입을 표시하는 인터럽트를 수신하면, 상기 연산 처리 장치는 인터럽트 타입에 대응하는 인터럽트 루틴을 실행하라는 명령을 표시하는 인터럽트를 상기 테이타 처리 장치에 출력하고, 상기 테이타 처리 장치는 상기 연산 처리 장치로부터 수신된 인터럽트에 의해 지정된 처리에 대응하는 인터럽트 루틴을 실행하는 것을 특징으로 하는 테이타 처리 방법.

청구항 44.

제42항에 있어서, 상기 데이터 처리 장치는 상기 연산 처리 장치로 인터럽트를 출력함으로써 처리의 결과를 보고하는 것을 특징으로 하는 데이터 처리 방법.

청구항 45.

제42항에 있어서, 상기 데이터 처리 장치는 상기 데이터 처리 장치 및 상기 연산 처리 장치에 의해 액세스 가능한 공통 메모리를 포함하고, 상기 연산 처리 장치는 풀링을 통해 상기 공통 메모리에 액세스함으로써 처리의 결과를 구하는 것을 특징으로 하는 데이터 처리 방법.

청구항 46.

제45항에 있어서, 상기 데이터 처리 장치는 상기 연산 처리 장치로부터의 인터럽트에 의해 요청된 처리의 실행 상태를 표시하는 제1 상태 레지스터에 플래그를 설정하고;

상기 연산 처리 장치는 상기 제1 상태 레지스터내의 플래그로부터 상기 데이터 처리 장치의 처리의 실행 상태를 판독하며;

상기 연산 처리 장치는 상기 연산 처리 장치가 인터럽트를 통해 처리를 실시하도록 상기 데이터 처리 장치에 요청하였는지 여부를 표시하는 제2 상태 레지스터에 플래그를 설정하며;

상기 데이터 처리 장치는 상기 연산 처리 장치가 상기 제2 상태 레지스터내의 플래그로부터 처리를 실시하도록 상기 데이터 처리 장치에 요청하였는지 여부를 판정하는 것을 특징으로 하는 데이터 처리 방법.

청구항 47.

제42항에 있어서, 상기 데이터 처리 장치는 초기 프로그램 및 인터럽트 루틴중 하나의 실행을 완료하면 저전력 상태로 들어가는 것을 특징으로 하는 데이터 처리 방법.

청구항 48.

제42항에 있어서, 상기 연산 처리 장치로부터 수신된 인터럽트에 근거하여, 상기 데이터 처리 장치는 콘텐츠 데이터의 구입 모드 및 사용 모드중 하나를 판정하는 처리와, 콘텐츠 데이터를 재생하는 처리와, 인증 기관으로부터 데이터를 다운로드하는 처리중 적어도 하나에 따라 인터럽트 루틴을 실행하는 것을 특징으로 하는 데이터 처리 방법.

청구항 49.

제42항에 있어서, 상기 연산 처리 장치는 선정된 사용자 프로그램을 실행하는 것을 특징으로 하는 데이터 처리 방법.

청구항 50.

연산 처리 장치, 제1 데이터 처리 장치, 및 제2 데이터 처리 장치를 사용하는 데이터 처리 방법에 있어서,

상기 연산 처리 장치에서, 선정된 프로그램을 실행하며, 마스터로서 작용함에 의해 선정된 조건에 따라 인터럽트를 출력하는 단계,

상기 제1 데이터 처리 장치에서, 슬레이브로서 작용함에 의해 상기 연산 처리 장치로부터 상기 인터럽트에 응답하여 조각 방지 모듈내의 콘텐츠 키 데이터로 암호화된 콘텐츠 데이터의 정상 처리를 수행하며, 상기 처리의 결과를 상기 연산 처리 장치에 리포트하는 단계, 및

상기 제2 데이터 처리 장치에서, 상기 제1 데이터 처리 장치내에서 상호 인증을 수행함에 의해 얻어진 상기 콘텐츠 키 데이터를 사용함에 의해 상기 콘텐츠 데이터를 해독하며, 상기 연산 처리 장치 또는 상기 제1 데이터 처리 장치용 슬레이브로서 작용함에 의해 상기 연산 처리 장치 또는 상기 제1 데이터 처리 장치로부터의 인터럽트에 응답하여 조작 방지 모듈내의 콘텐츠 데이터를 압축 또는 압축해제하는 단계

를 포함하는 데이터 처리 방법.

청구항 51.

연산 처리 장치, 제1 데이터 처리 장치 및 제2 데이터 처리 장치를 사용하는 데이터 처리 방법에 있어서,

상기 연산 처리 장치에서, 선정된 프로그램을 실행하며, 마스터로서 작용함에 의해 선정된 조건에 따라 인터럽트를 출력하는 단계,

상기 제1 데이터 처리 장치에서, 슬레이브로서 작용함에 의해 상기 연산 처리 장치로부터 상기 인터럽트에 응답하여 조작 방지 모듈내의 콘텐츠 키 데이터로 암호화된 콘텐츠 데이터의 정상 처리를 수행하며, 상기 처리의 결과를 상기 연산 처리 장치에 리포트하는 단계, 및

상기 제2 데이터 처리 장치에서, 상기 연산 처리 장치로 상호 인증을 수행하며, 상기 연산 처리 장치로부터의 상기 인터럽트에 응답하여 조작 방지 모듈내의 기록 매체로/로부터 상기 콘텐츠 데이터를 판독 및 기록하는 단계

를 포함하는 데이터 처리 방법.

청구항 52.

제51항에 있어서, 상기 제2 데이터 처리 장치는 상기 기록 매체에 대응하는 매체 키 데이터를 사용함에 의해 상기 콘텐츠 데이터를 해독 및 암호화하는 데이터 처리 방법.

청구항 53.

제51항에 있어서, 상기 기록 매체가 상호 인증 기능을 갖는 처리 회로를 구비할 때, 상기 제2 데이터 처리 장치는 상기 처리 회로로 상호 인증을 수행하는 데이터 처리 방법.

청구항 54.

연산 처리 장치, 제1 데이터 처리 장치, 및 제2 데이터 처리 장치를 사용하는 데이터 처리 방법에 있어서,

상기 연산 처리 장치에서, 선정된 프로그램을 실행하며, 마스터로서 작용함에 의해 선정된 조건에 따라 인터럽트를 출력하는 단계,

상기 제1 데이터 처리 장치에서, 상기 연산 처리 장치로 상호 인증을 수행하며, 상기 연산 처리 장치로부터의 인터럽트에 응답하여 조작 방지 모듈내의 기록 매체로/로부터 콘텐츠 데이터를 판독 및 기록하는 단계, 및

상기 제2 데이터 처리 장치에서, 콘텐츠 키 데이터를 사용함에 의해 상기 콘텐츠 데이터를 해독하며, 상기 연산 처리 장치용 슬레이브로서 작용함에 의해 상기 연산 처리 장치로부터의 인터럽트에 응답하여 조작 방지 모듈내의 상기 콘텐츠 데이터를 압축 또는 압축해제하는 단계

를 포함하는 데이터 처리 방법.

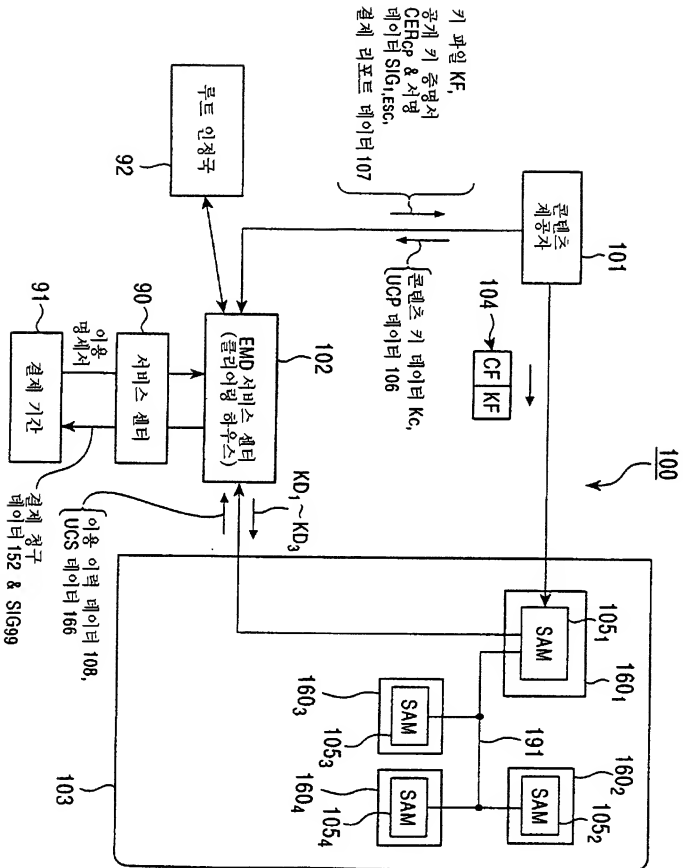
청구항 55.

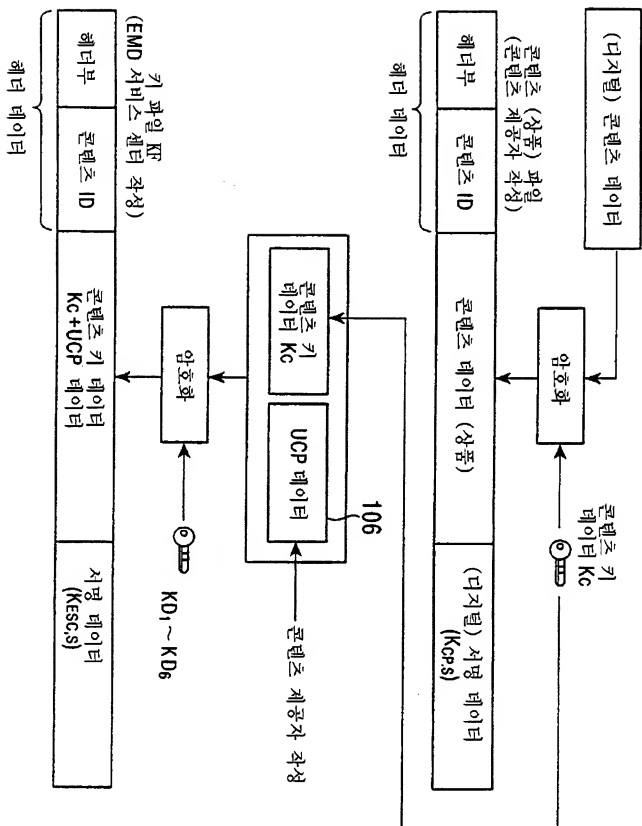
제54항에 있어서, 상기 제1 데이터 처리 장치에 의해 상기 기록 매체로부터 판독된 상기 콘텐츠 데이터가 저장 회로에 일시적으로 저장되며, 상기 저장 회로로부터 판독된 상기 콘텐츠 데이터는 상기 제2 데이터 처리 장치에 출력되는 데이터 처리 방법.

청구항 56.

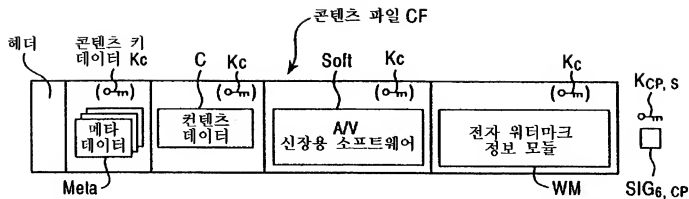
제55항에 있어서, 상기 저장 회로는 반전동 저장 회로의 저장 영역의 일부를 사용하는 데이터 처리 방법.

도면

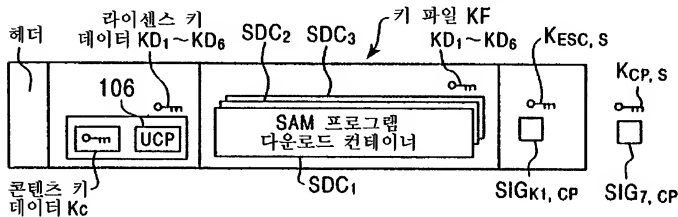




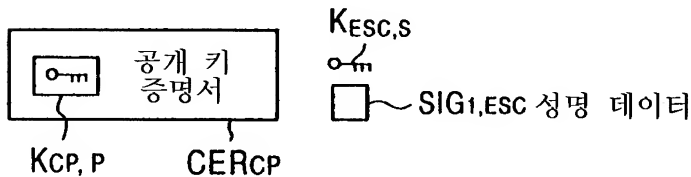
도면 3a

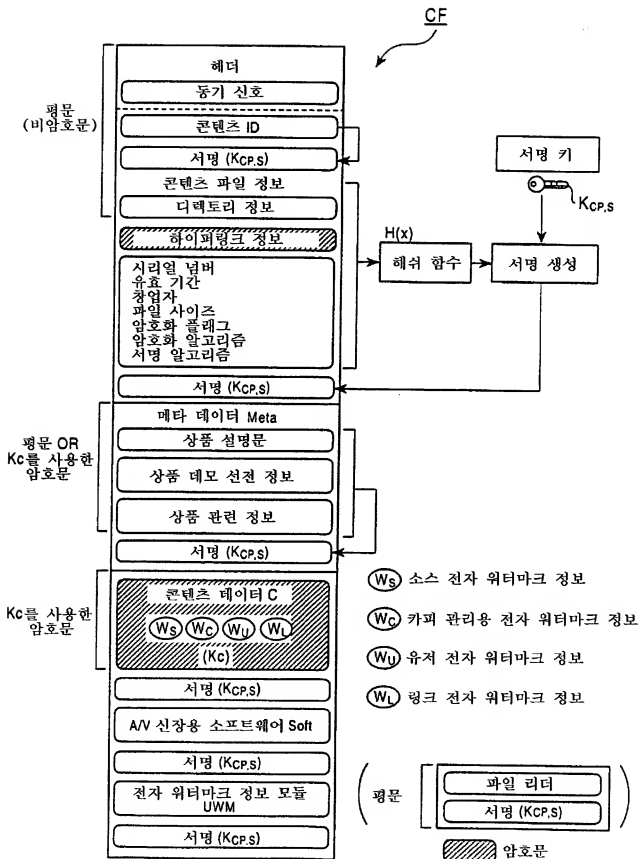


도면 3b

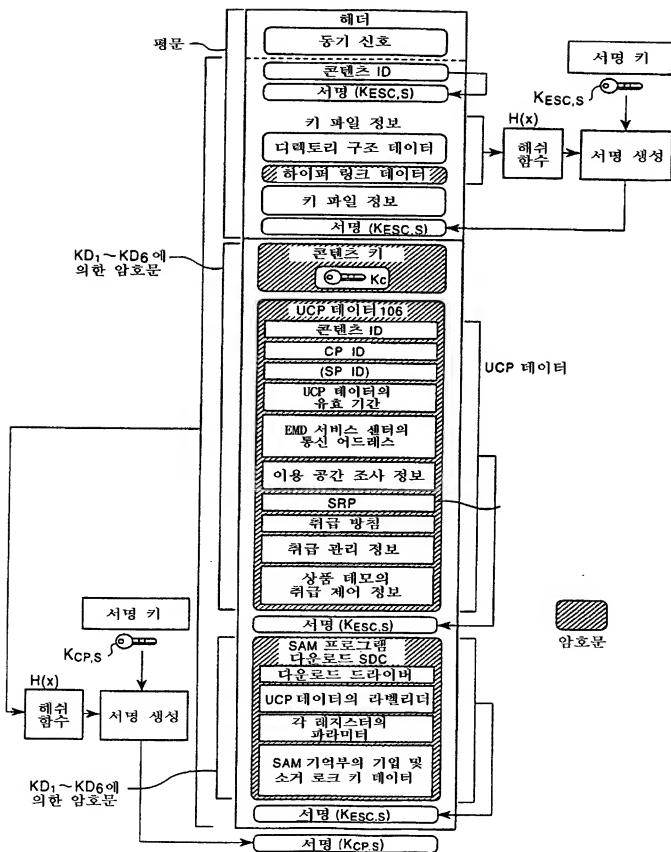


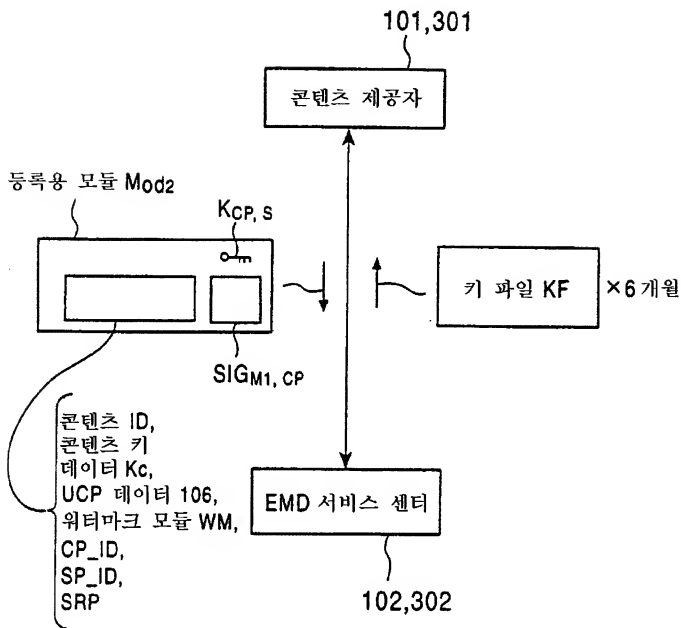
도면 3c





도면 5

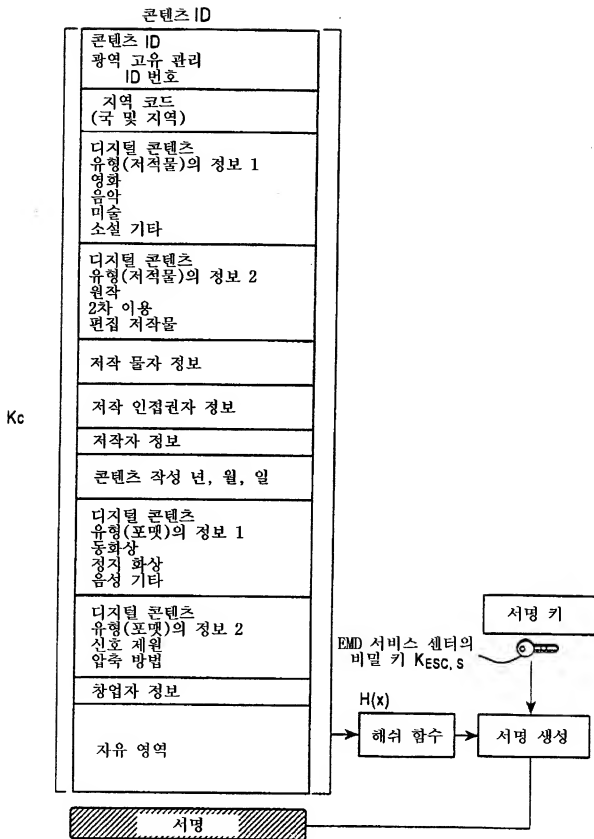


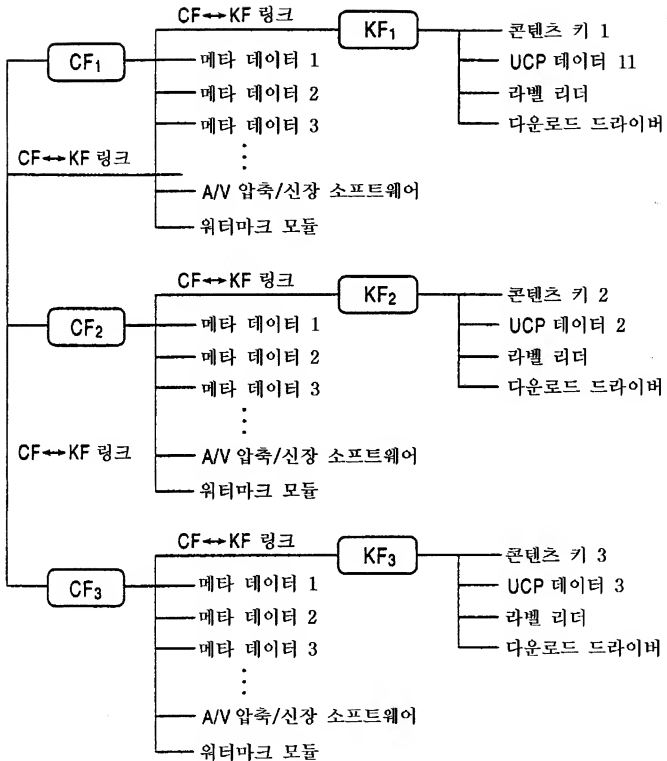


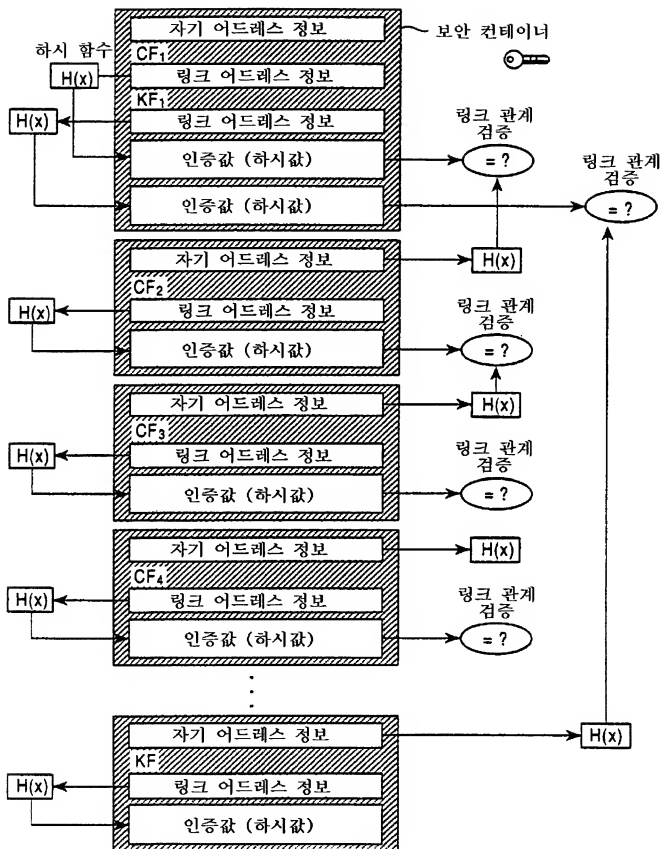
헤더 데이터

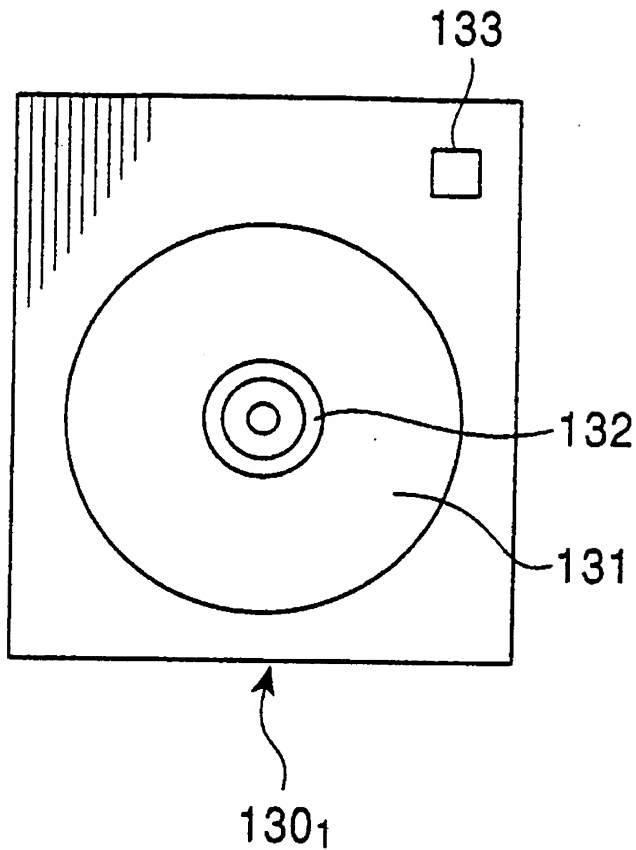
헤더	콘텐츠 ID	디지털 콘텐츠	디지털 서명
----	--------	---------	--------

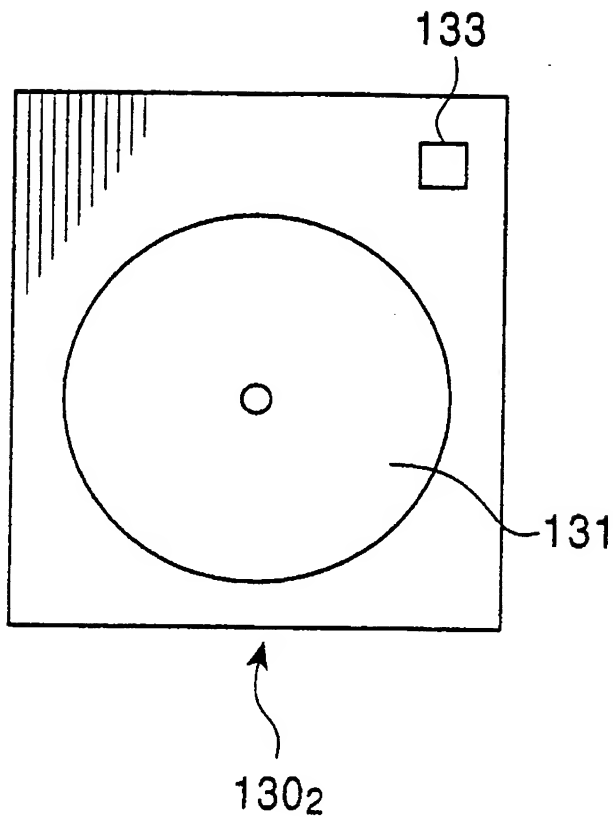
동기 신호
헤더 길이
패킷 길이
<p>보안 컨테이너 정보</p> <ol style="list-style-type: none"> 1. 시리얼 넘버 2. 유효 기간 3. 창업자 4. 파일 사이즈 5. 암호 플래그 6. 암호 알고리즘 7. 서명 알고리즘 <p>디지털 콘텐츠의 유형</p> <p>음성 (곡)</p> <p>영상 (비디오 클립)</p> <p>텍스트 1 (뮤직 카드)</p> <p>텍스트 2 (라이너 노트)</p> <p>정지 화상 (재킷)</p> <p>앨범</p> <p>요소 (단일체)</p> <p>가격 데이터</p> <p>UCP 데이터</p>

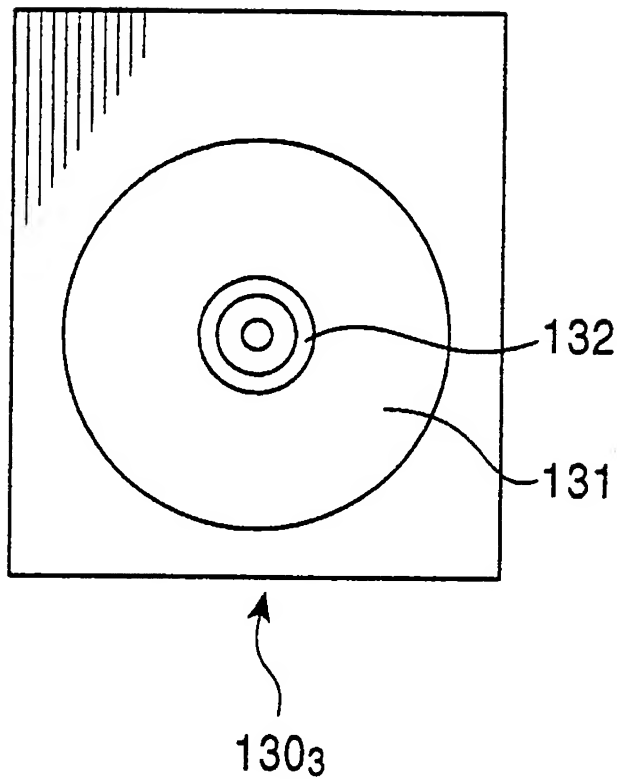


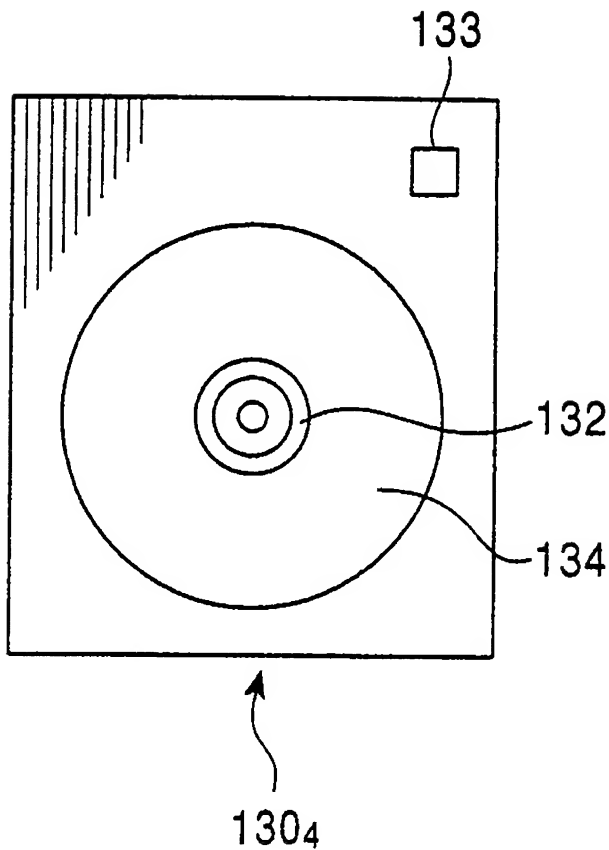


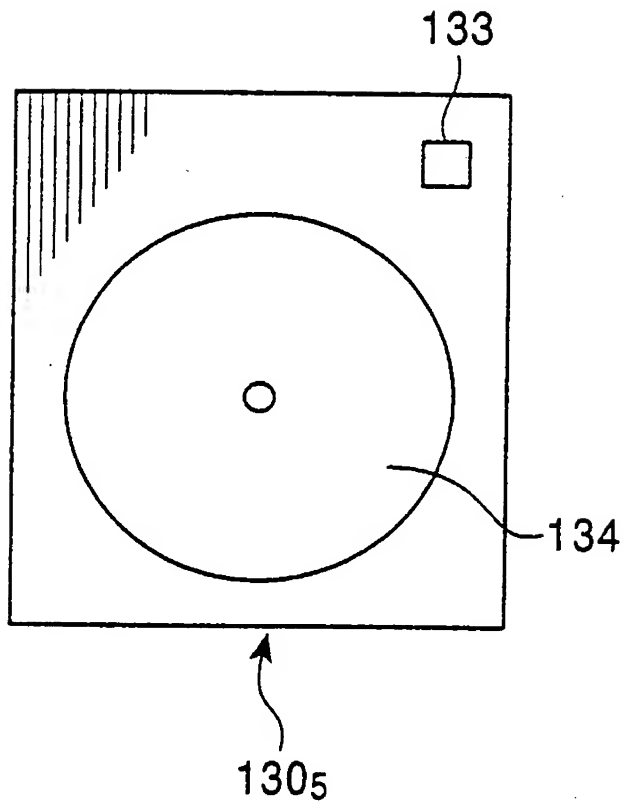




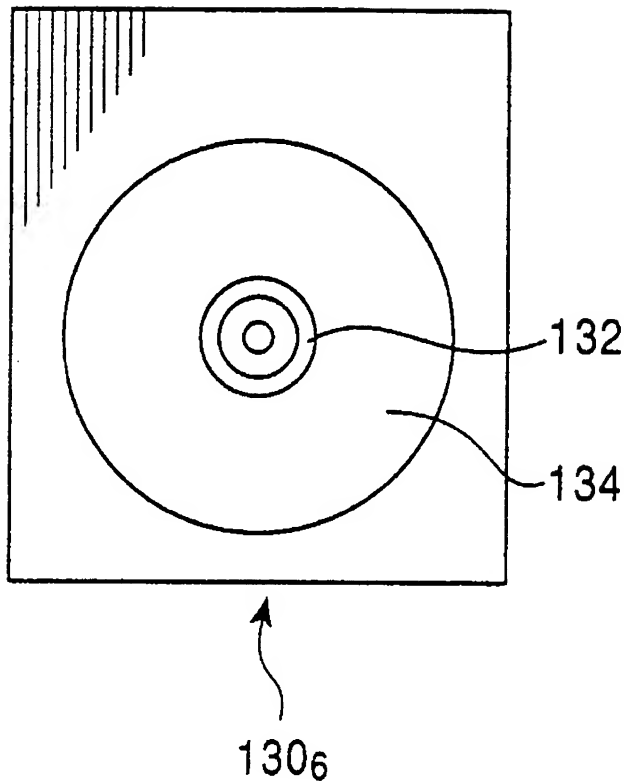








도면 16



콘텐츠 제공자의
보안 컨테이너

S17-1

ESC로부터 공개 키 인증서를 입수

S17-2

콘텐츠 마스터 소스를 디지털화함
IDS를 할당함
콘텐츠 마스터 소스 데이터베이스내에 저장

S17-3

각 콘텐츠에 대해 메타 데이터 작성하고
메타 데이터 베이스에 저장

S17-4

디지털 워터마크 정보(워터마크)를
콘텐츠 데이터(워터마크 인코딩)로 삽입

검출
실패

워터마크 검출
(워터마크 디코딩)

S17-9

검출 성공

S17-5

콘텐츠 및 워터마크 삽입 위치를
데이터 베이스에 저장

신장된 콘텐츠 데이터의
음성 검출을 실행

S17-8

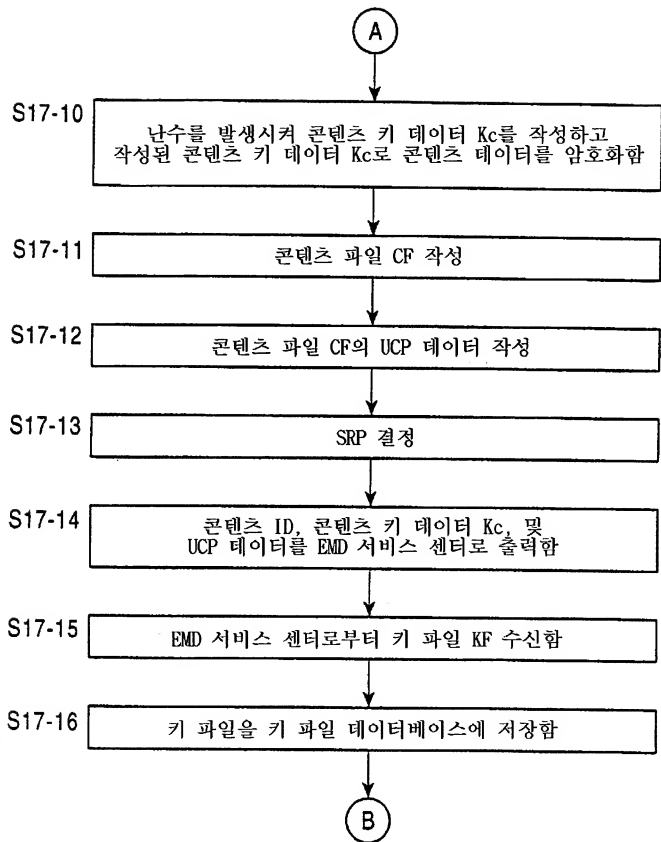
S17-6

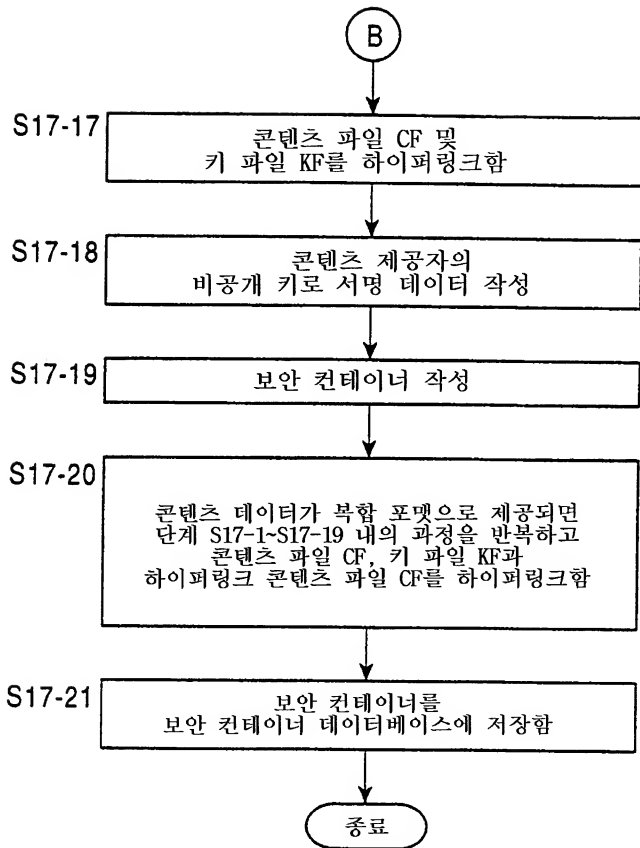
콘텐츠 데이터 압축

콘텐츠 데이터 신장

S17-7

A





라이선스 키 데이터를
콘텐츠 제공자와 SAM에 공급함

공개 키 증명서 데이터
CER_{CP}, CER_{SAM1}~CER_{SAM4}를
발행함

키 파일 KF 작성

이용 이력 데이터에 기초하여
결제 처리(이익 분배 처리)를 실행함

ESC_ 콘텐츠 ID

CP_ 콘텐츠 ID

(SP_ 콘텐츠 ID)

유저 ID

유저 정보

SAM_ID

HNG_ID

디스카운트 정보

트레이싱 정보

(가격 데이터 PT)

CP_ID

(SP_ID)

서비스 제공자 (포털) ID

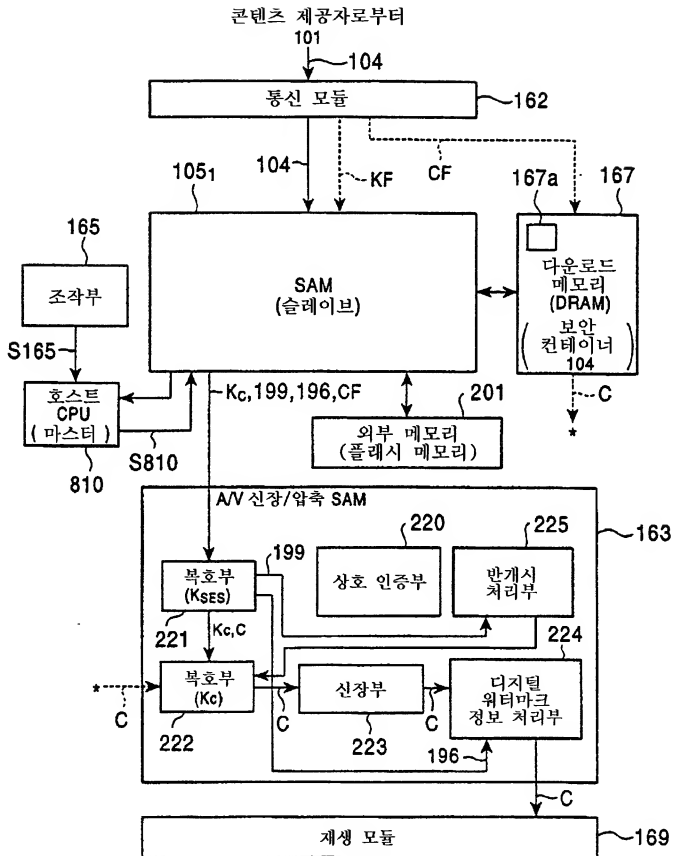
하드웨어 제공자

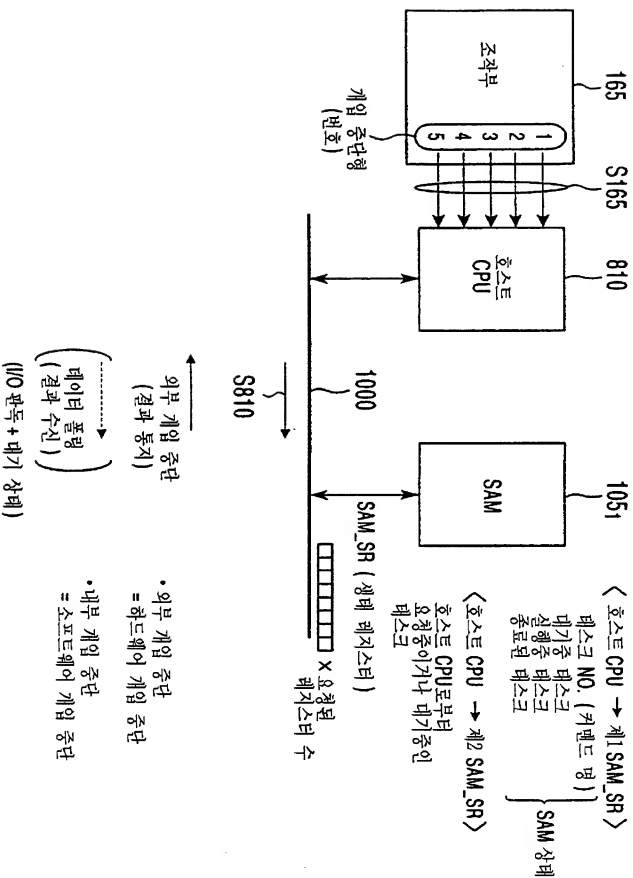
MEDIA_ID

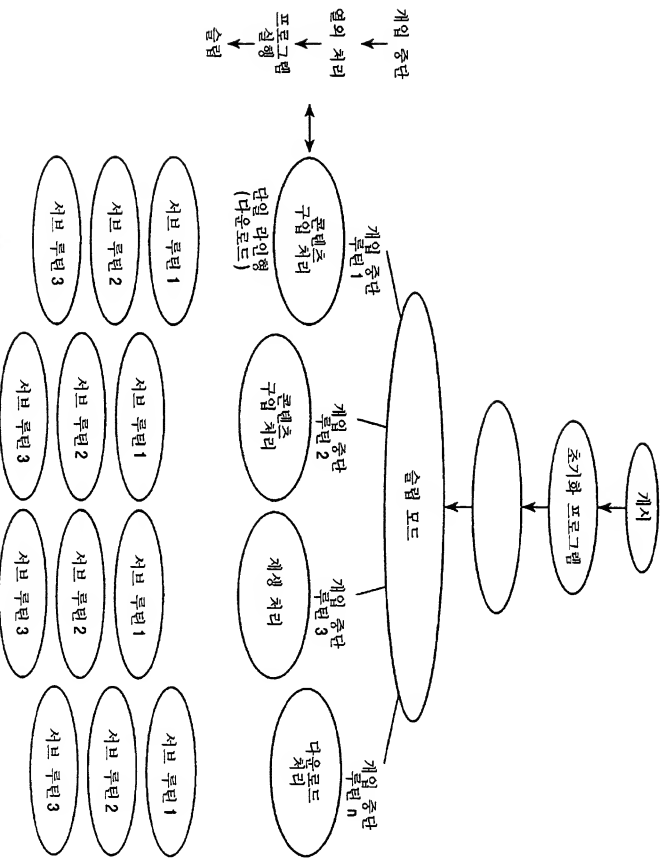
컴포넌트 ID

라이센스 소유자 LH_ID의 식별자

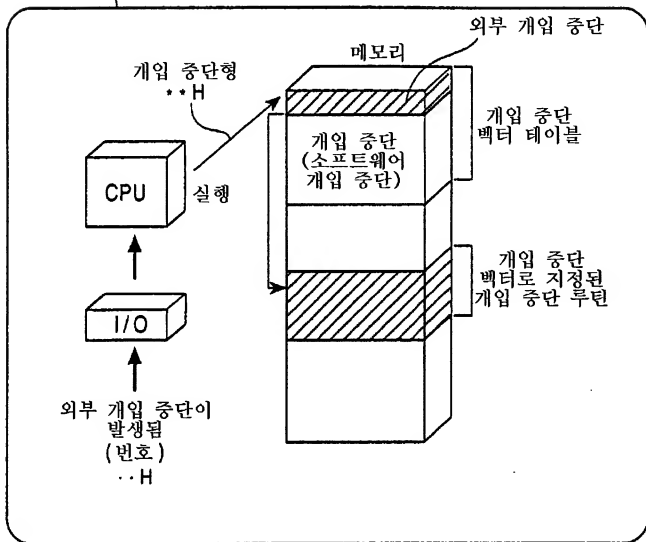
ESC_ID

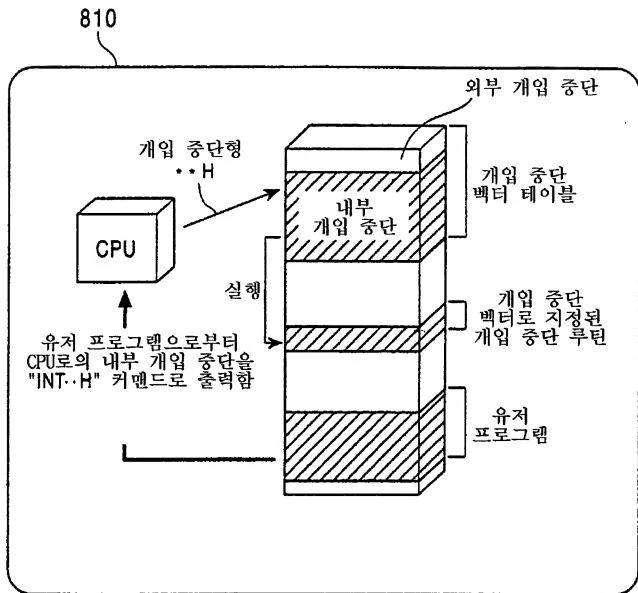


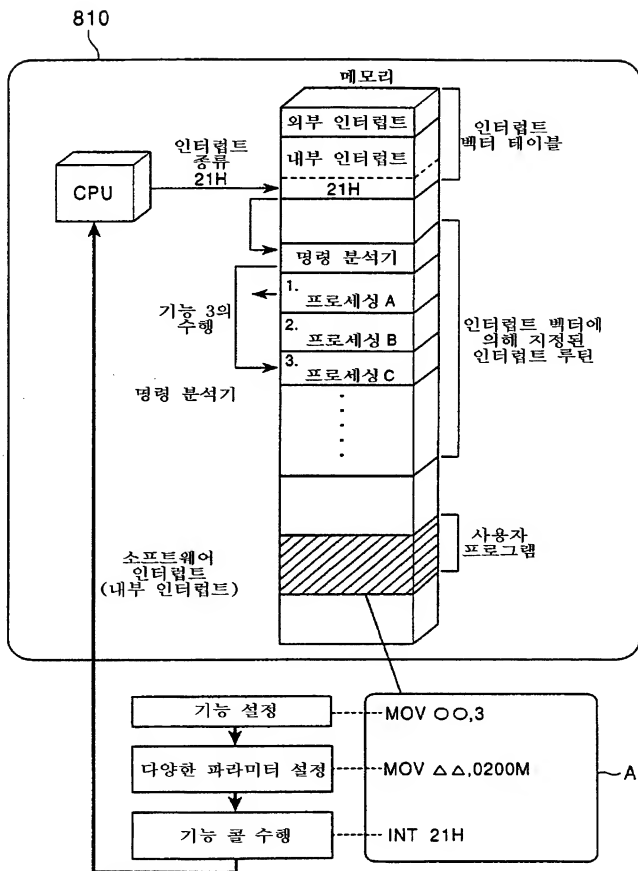


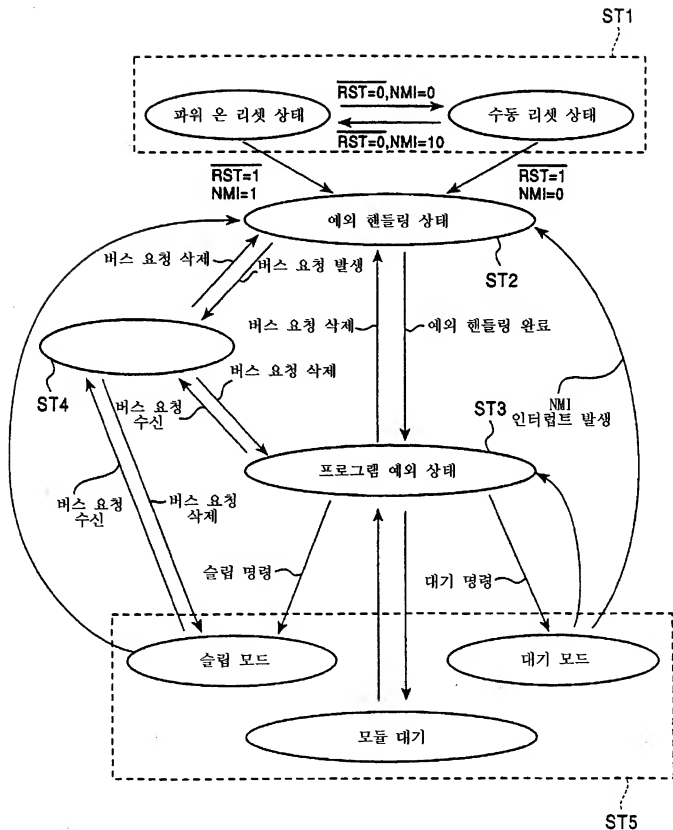


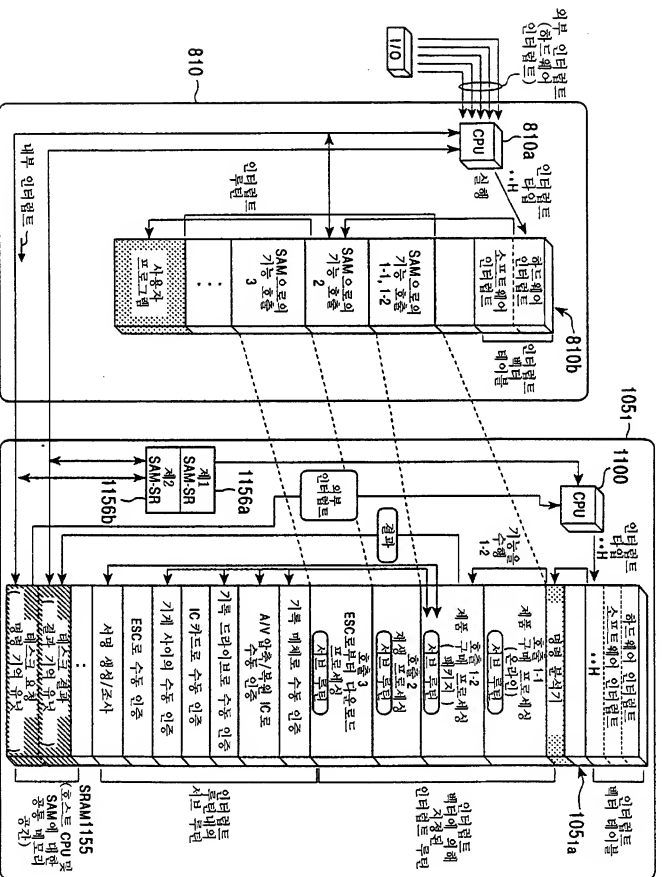
810

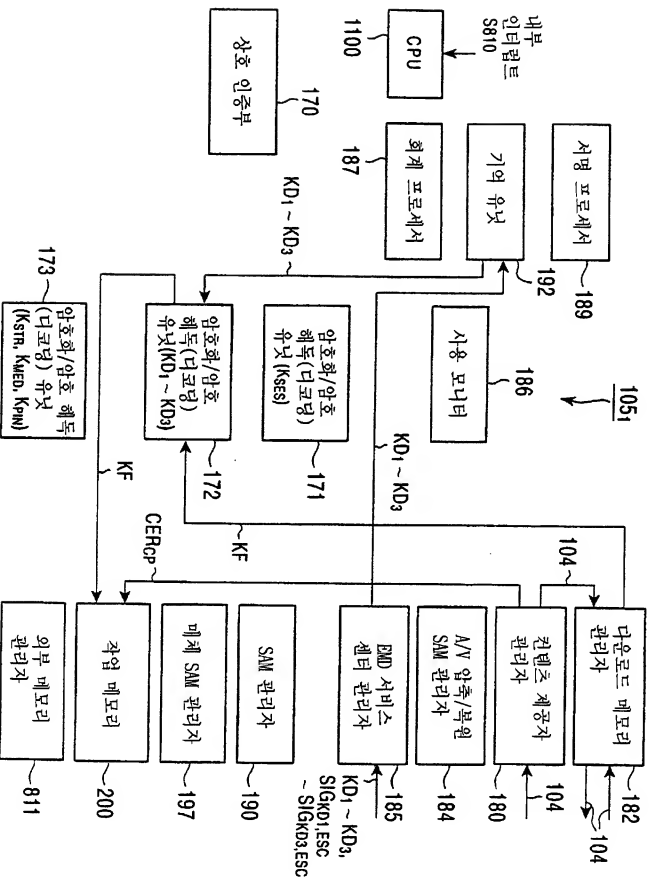












이용 로그 데이터 108

SAM 등록 리스트

(KF: 다운로드 메모리에 SAM이 없는 경우)

컨텐츠 키 데이터 K_c

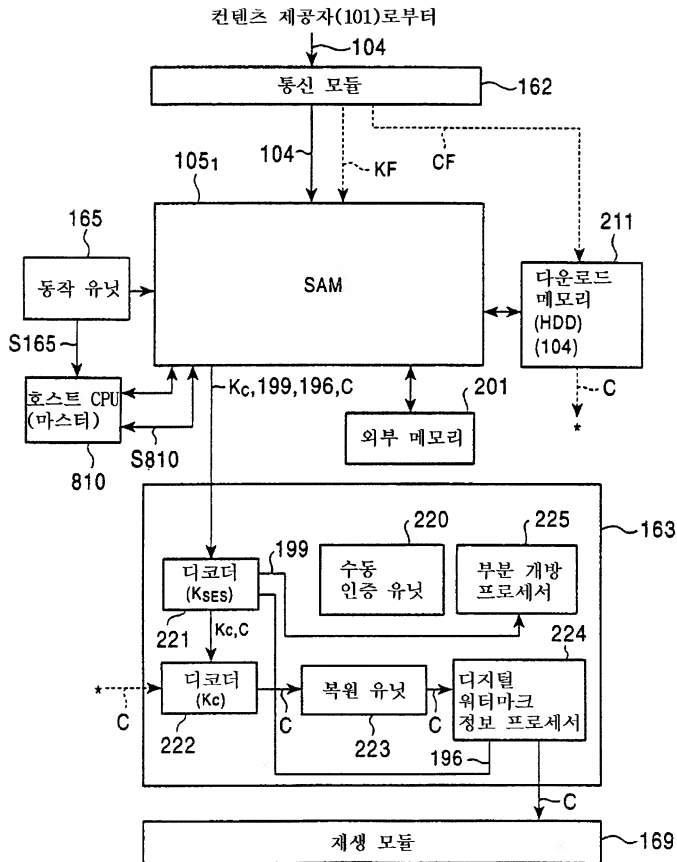
UCP 데이터 106














저장 유닛 192의 록 키 데이터 K_{Loc}

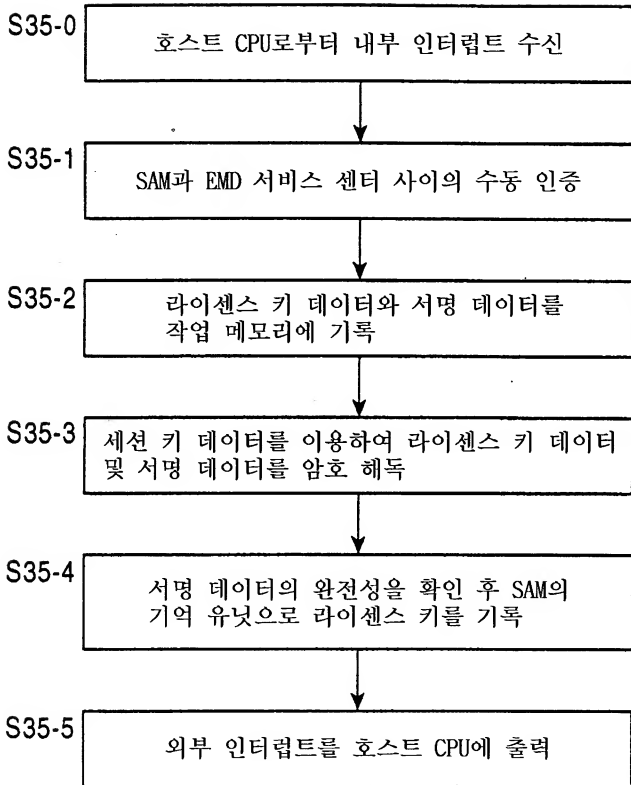
컨텐츠 제공자의 공개 키 증명서 CER_{CP}

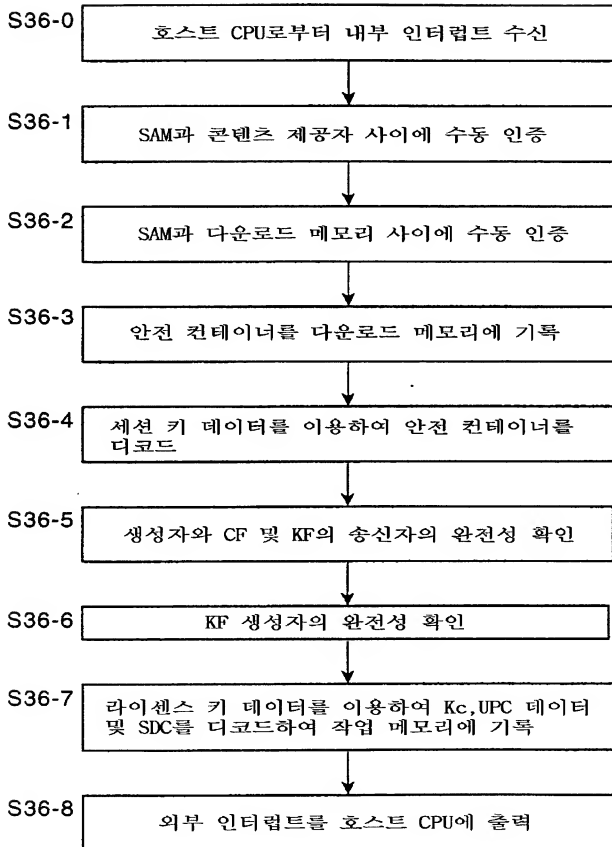
UCS 데이터 166

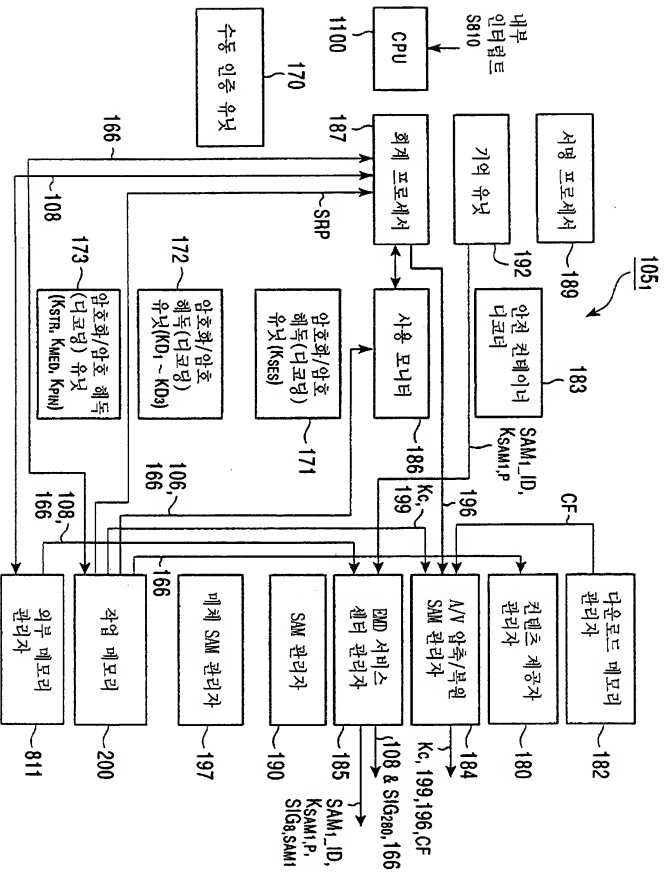
SAM 프로그램 다운로드 컨테이너 $SDC_1 \sim SDC_3$

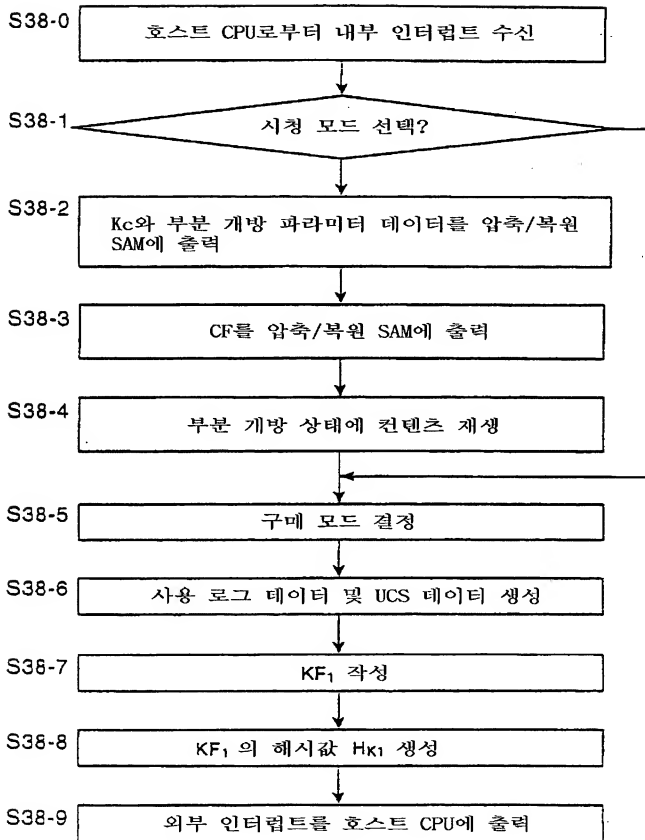


★	SAM_ID	<p>라이선스 키 KD₁ ~ KD₃ (64 BITS)</p>
	사용자_ID	
	패스워드	
★	HNG_ID	
	정보 참조 ID	
	SAM 등록 리스트	
	최소 리스트 (기계 및 기록 매체)	
★	(기억 키 K _{STR} )	
★	MAC 키 K _{MAC} 	
★	루트 CA의 공개 키 K _{FCA}	
★	ESC 공개 키 (160BITS → 192BITS) 	
구동 SAM & 구동 SAM의 공개 키에 대한 소스 키 데이터 (X, 509)		
<p>*** SAM 개인 키-공개 키 ***</p> <p>SAM 개인 키  K_{SAM1,S} K_{SAM1,P} CER_{SAM1}</p> <p>SAM 공개 키 증명 (X, 509)  SAM 공개 키  K_{ESC,S}  SIG_{22,ESC}</p>		
★	A/V 압축/복원 SAM을 갖는 인증에 대한 소스 키 데이터 (40 ~ 64 BITS)	 (공통 키 암호 작성 체계를 이용한 경우)
★	<p>• 매체 SAM을 같은 소스 키 데이터 (40 ~ 64 BITS)</p> <p>• 매체 SAM의 공개 키 증명 (X.509)</p> <p>수동 인증에 의해 매체 SAM으로부터 SAM으로 보냄 (160 ~ 192 BITS)</p>	<p> (공통 키 암호 작성 체계를 이용한 경우)</p> <p>K_{MEDSAM} CER_{MEDSAM}  K_{ESC,S}  SIG</p> <p> 매체 SAM의 공개 키 </p>
★	취급될 수 있는 신호 소스	
★	권리 처리용 데이터 이력 분배하는 엔티티 ID	

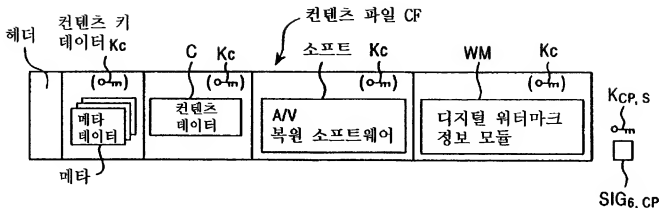




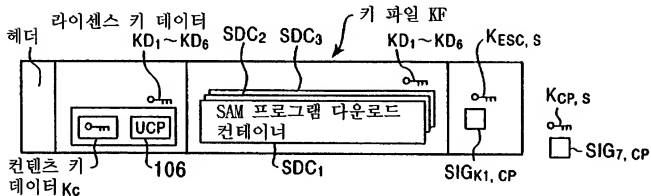




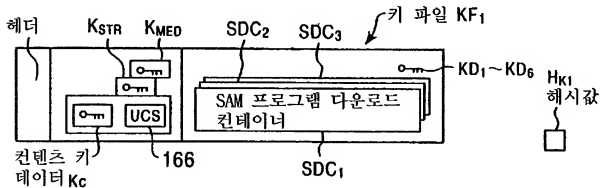
도면 39a



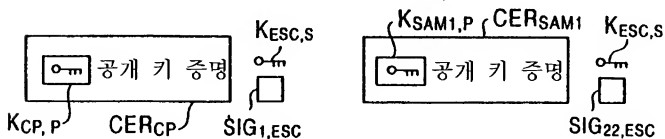
도면 39b

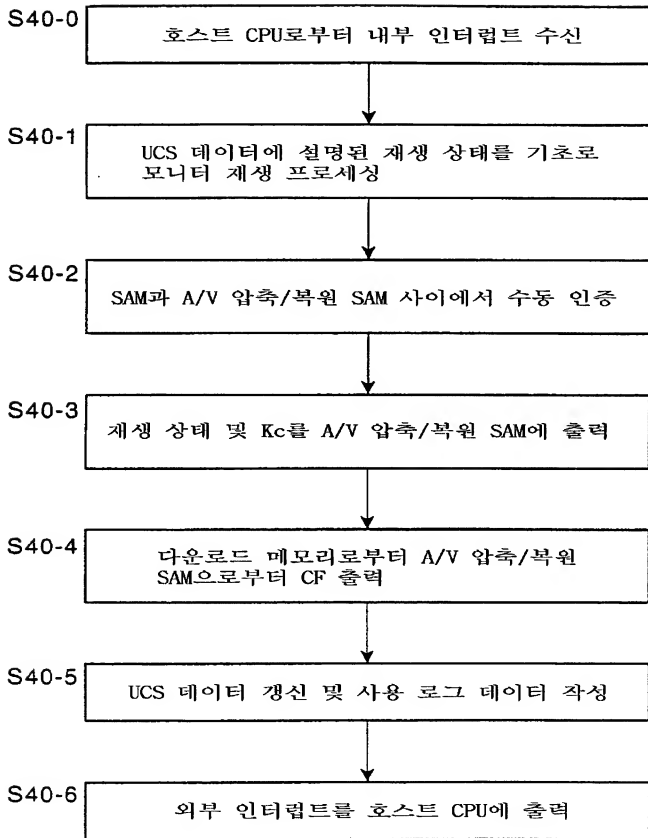


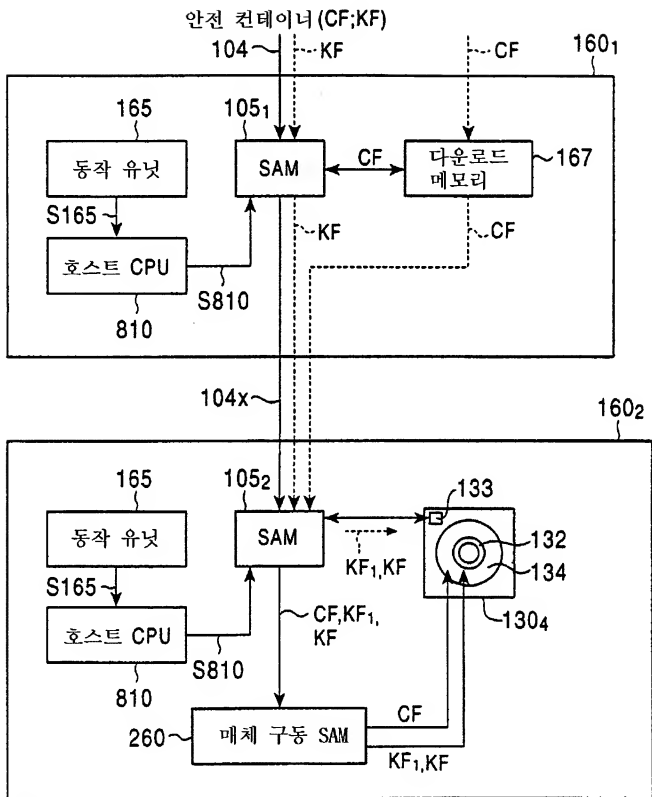
도면 39c

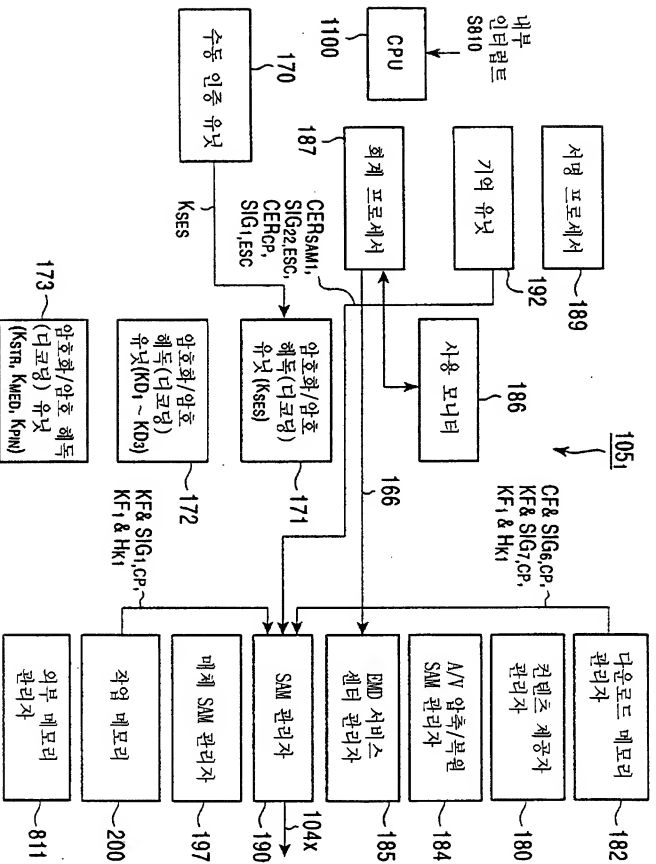


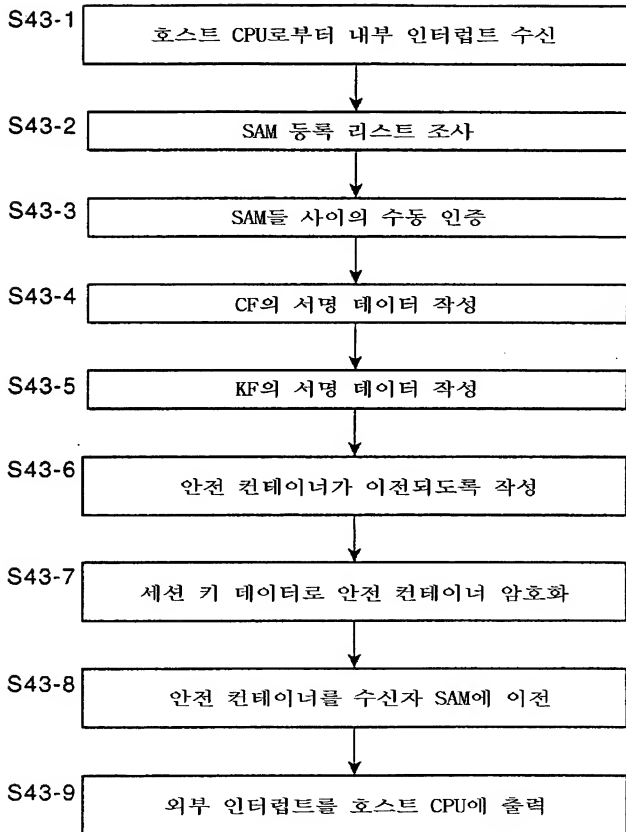
도면 39d



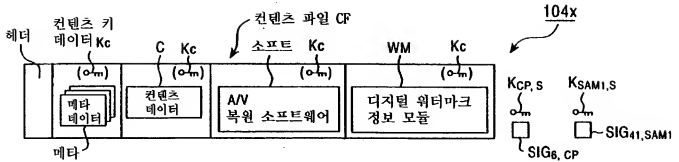




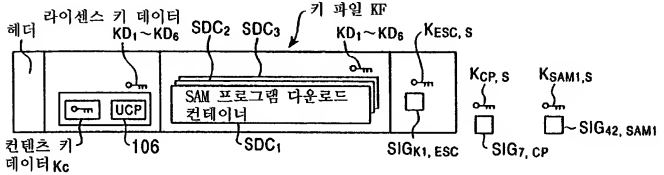




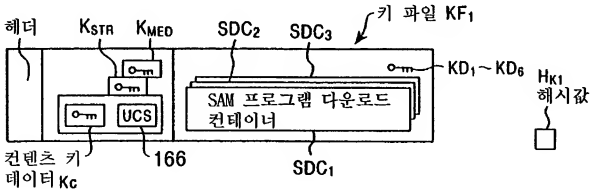
도면 44a



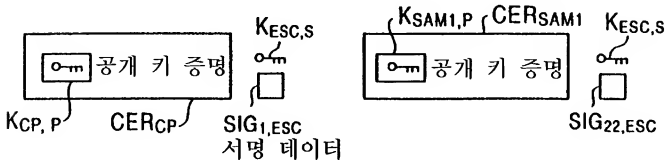
도면 44b

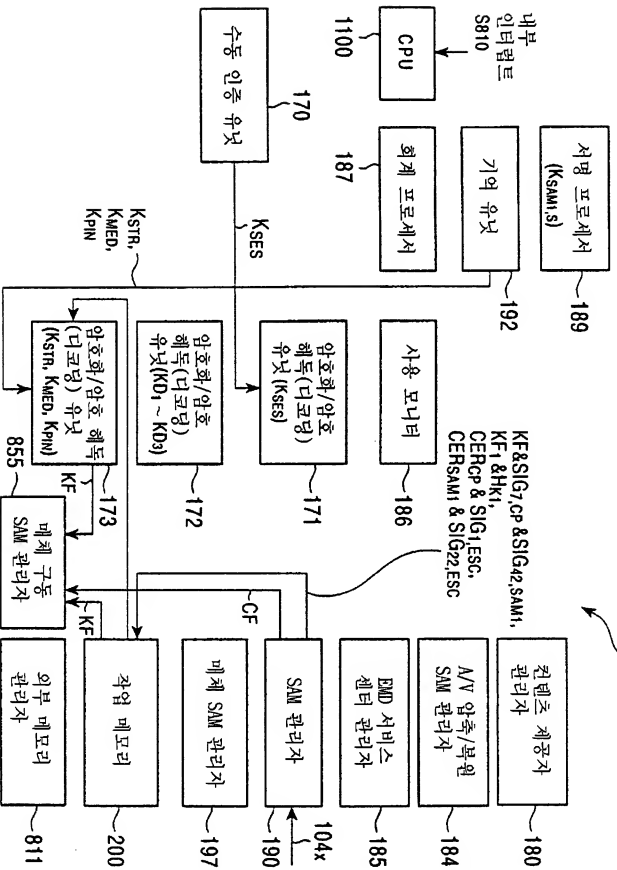


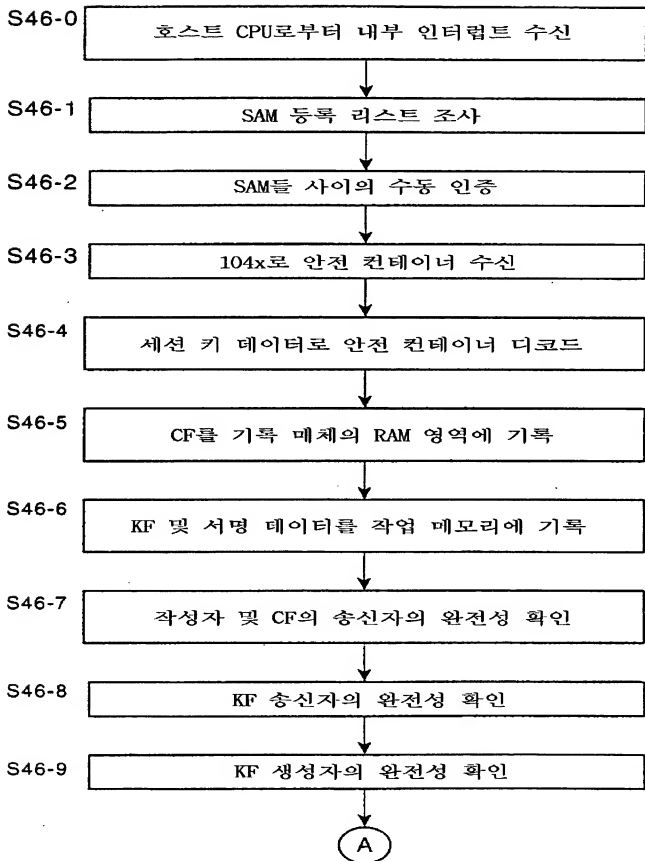
도면 44c

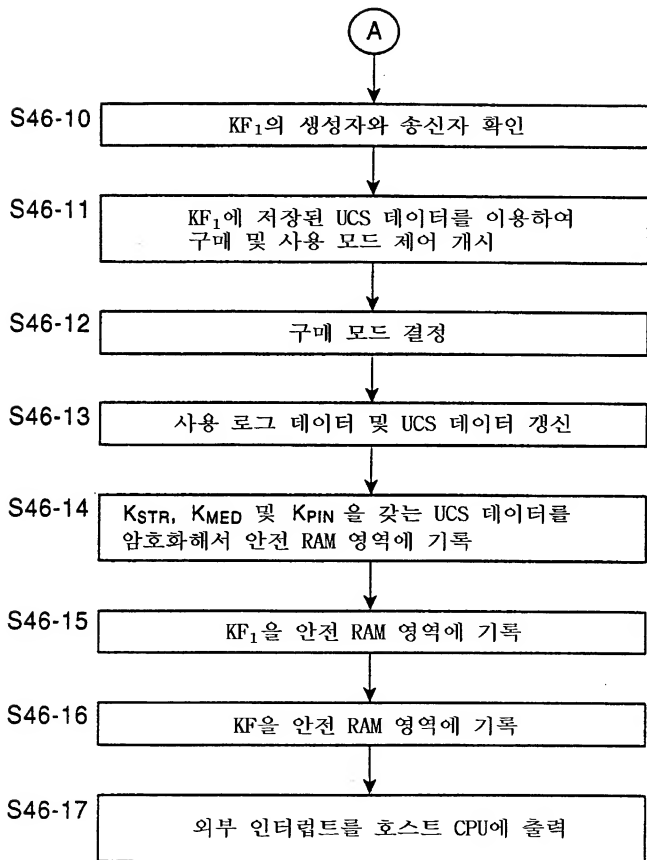


도면 44d



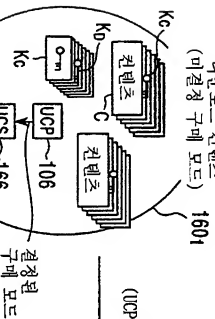






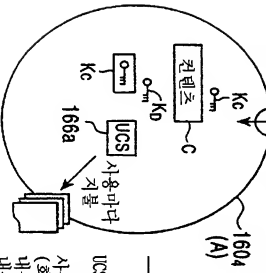
네트워크 장치 및 홈 서버

다운로드 콘텐츠
(미결정 구매 모드)



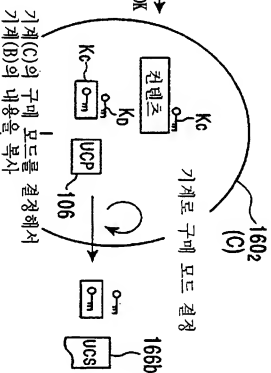
홈 서버의 구매 모드를
결정하고 휴대용 장치에
콘텐츠 전달

전달 UCS로부터 구매



재분배
(UCP로부터 구매)

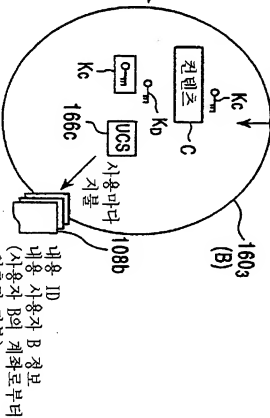
복사 OK



가게(C)의 구매 모드를 결정해서
가게(B)의 내용을 복사

복사

1603 (B)



구매 모드가 결정된
내용을 구매

복사 OK

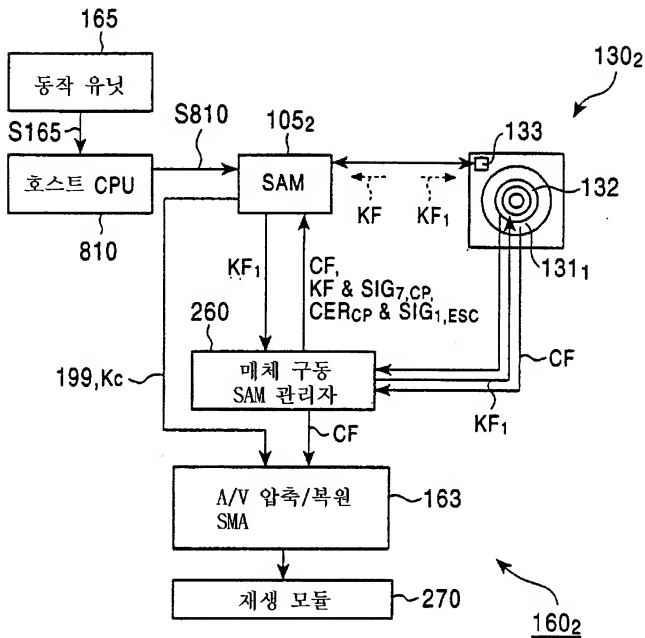
UCS로부터 구매

사용 로그 데이터 108a
(회계 정보)

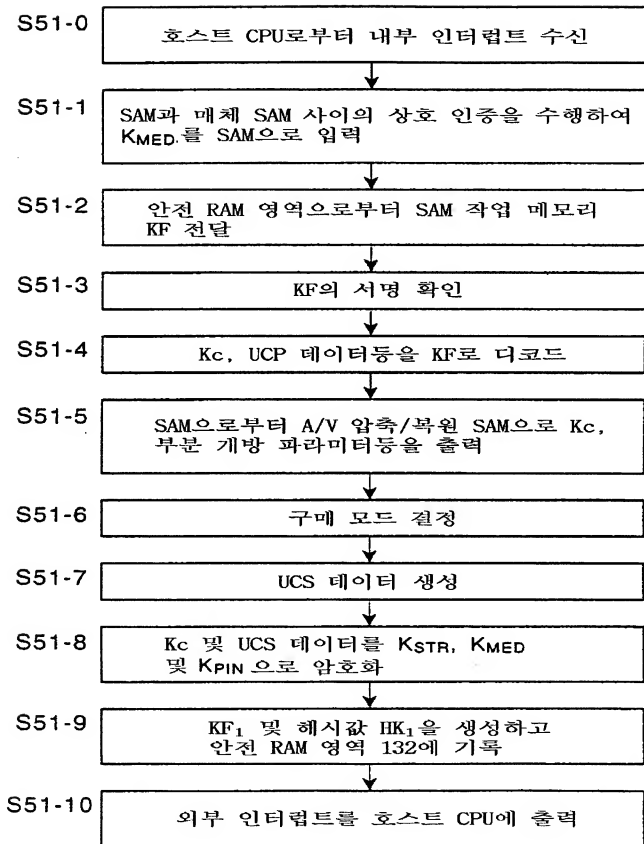
내용 ID

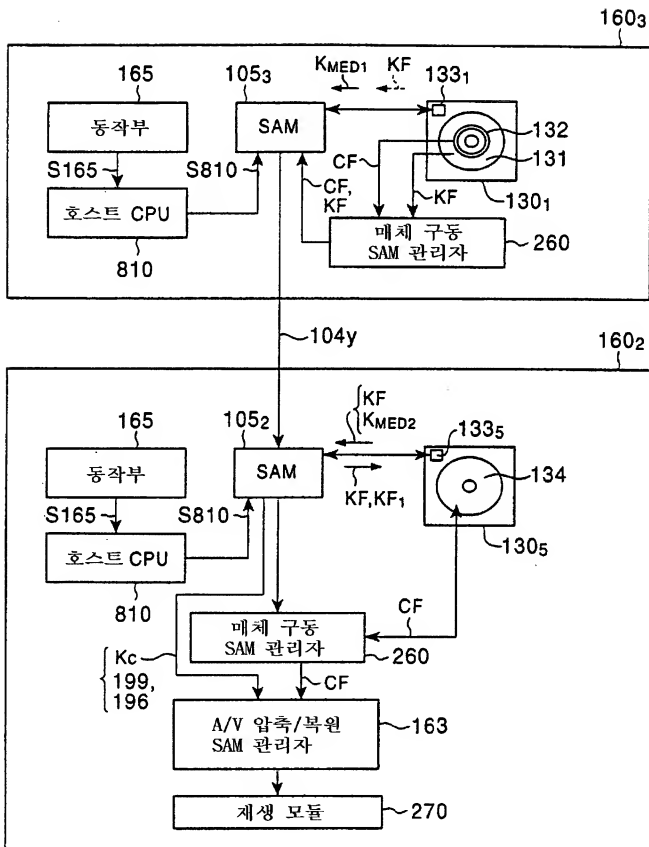
내용 사용자 A 정보

(사용자 A의 계좌로부터 인출된 지불)

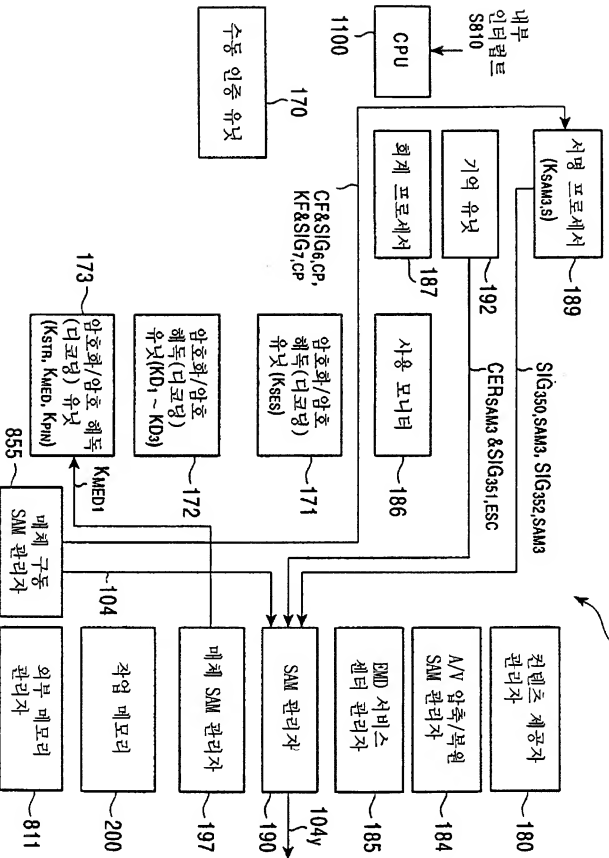




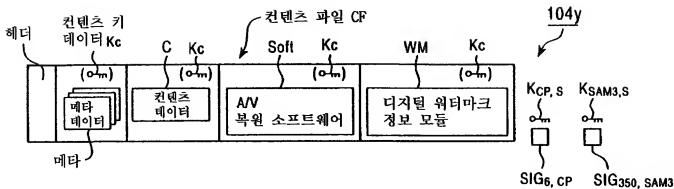




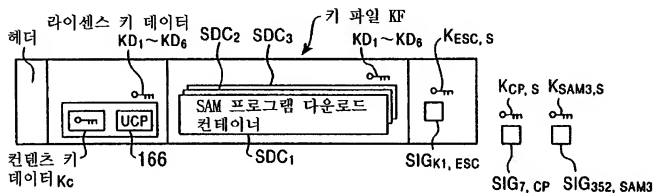
1053



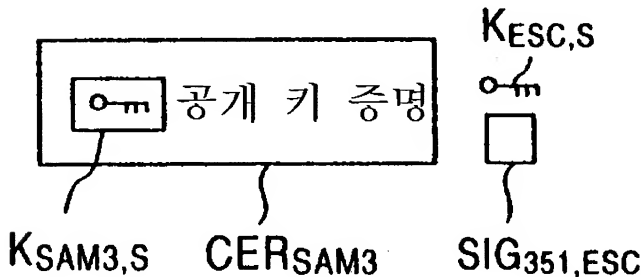
도면 54a

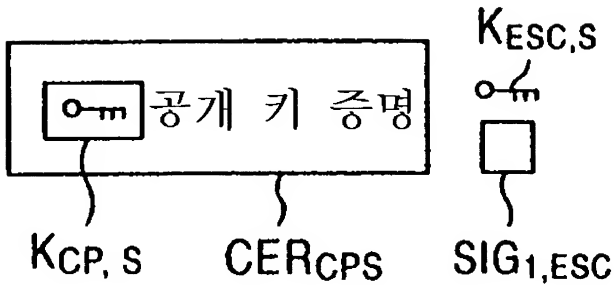


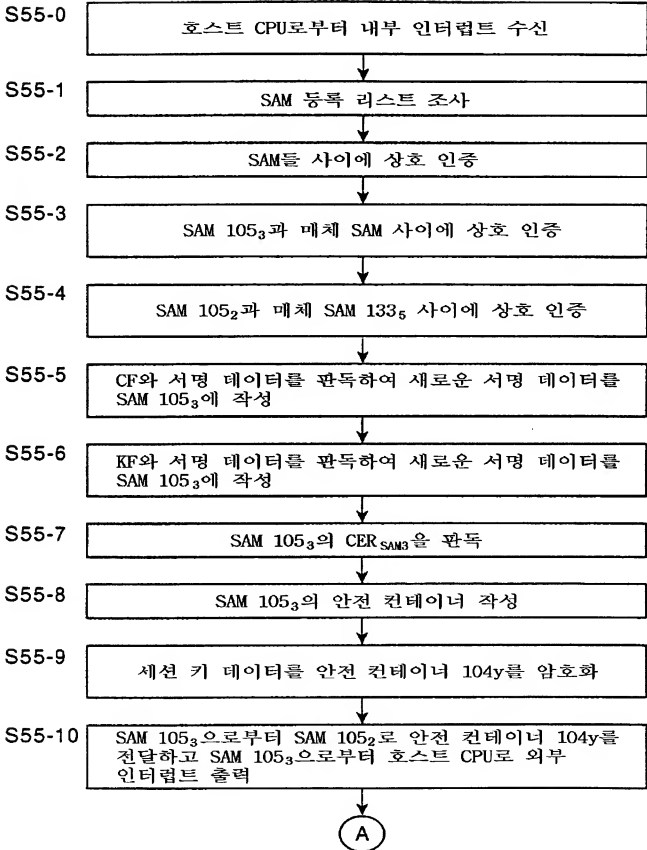
도면 54b

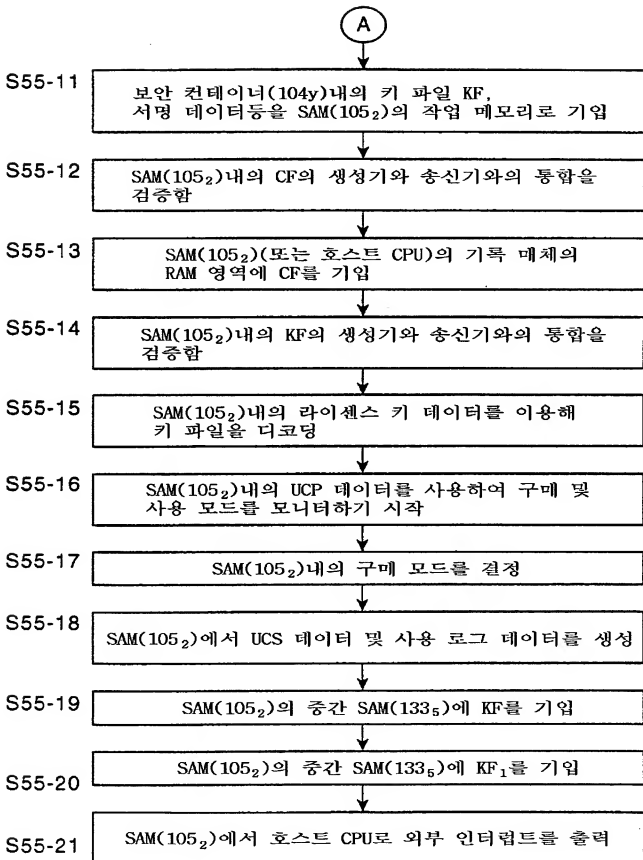


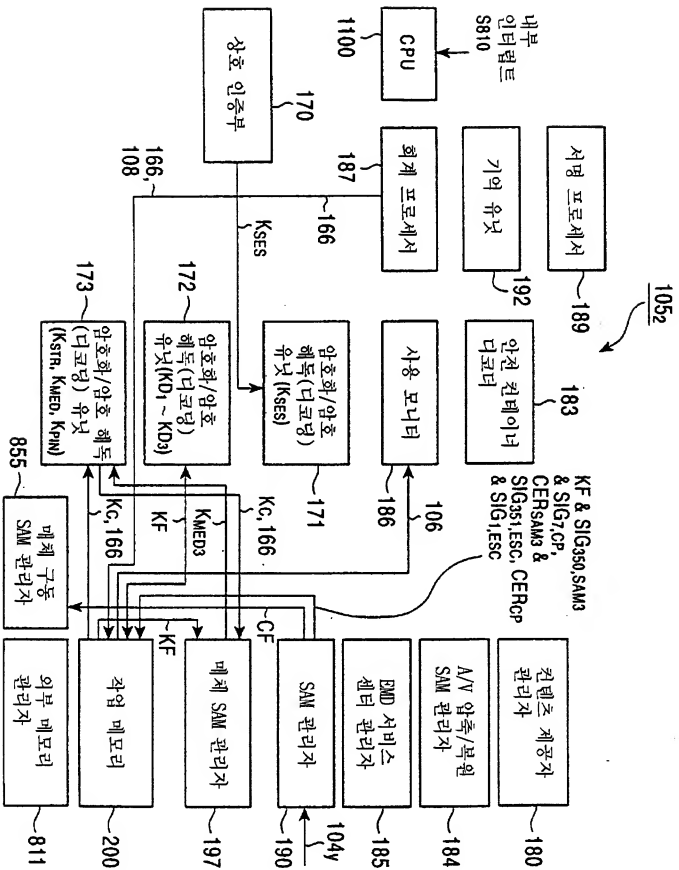
도면 54c

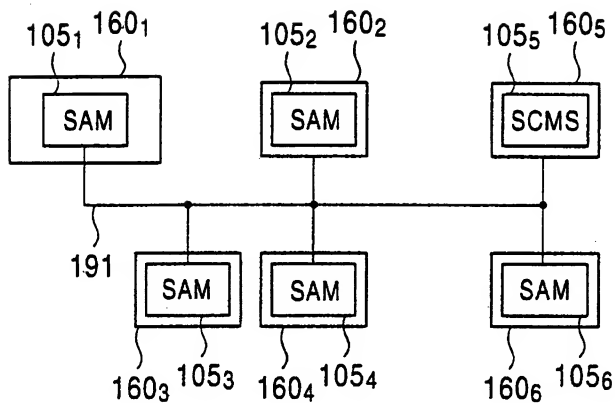


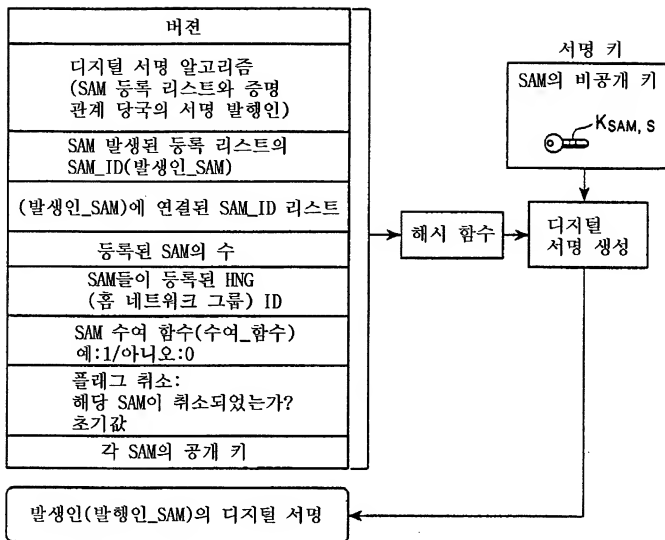




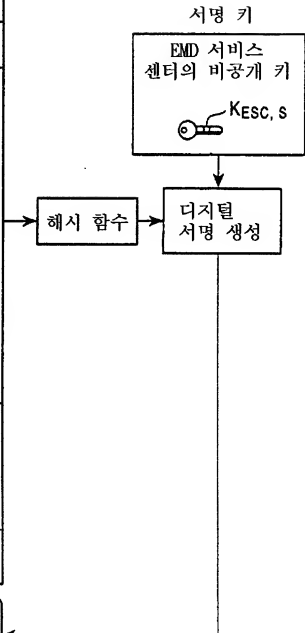
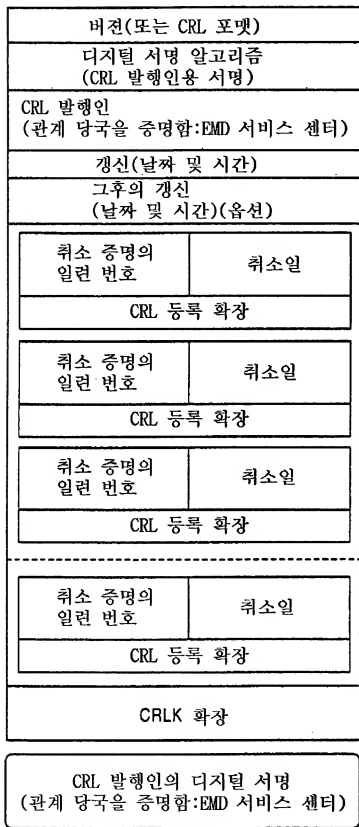


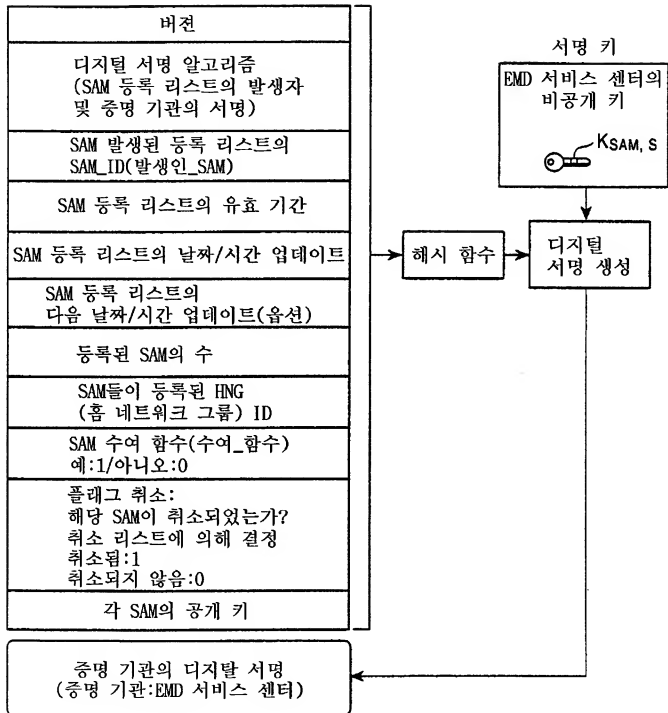


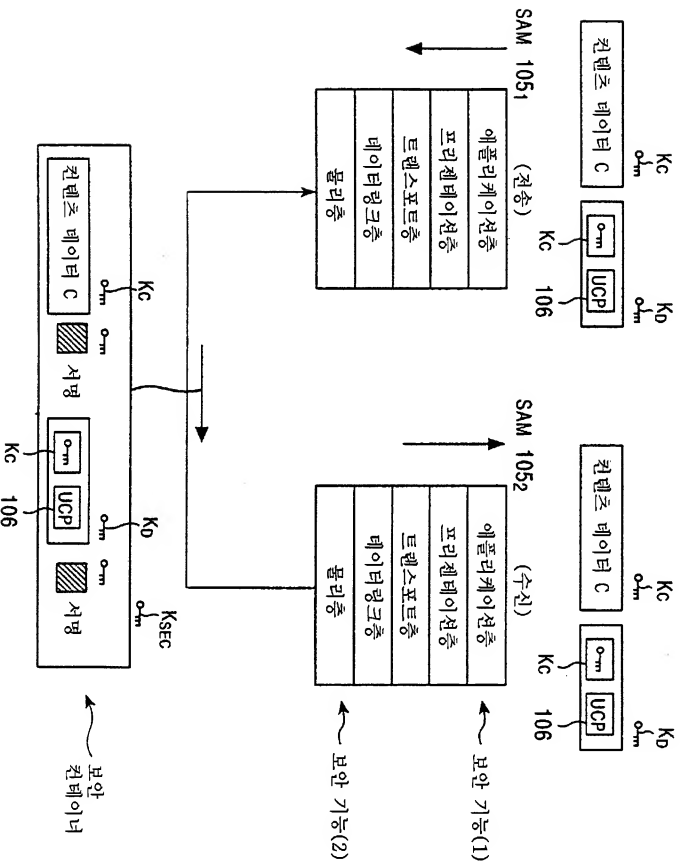


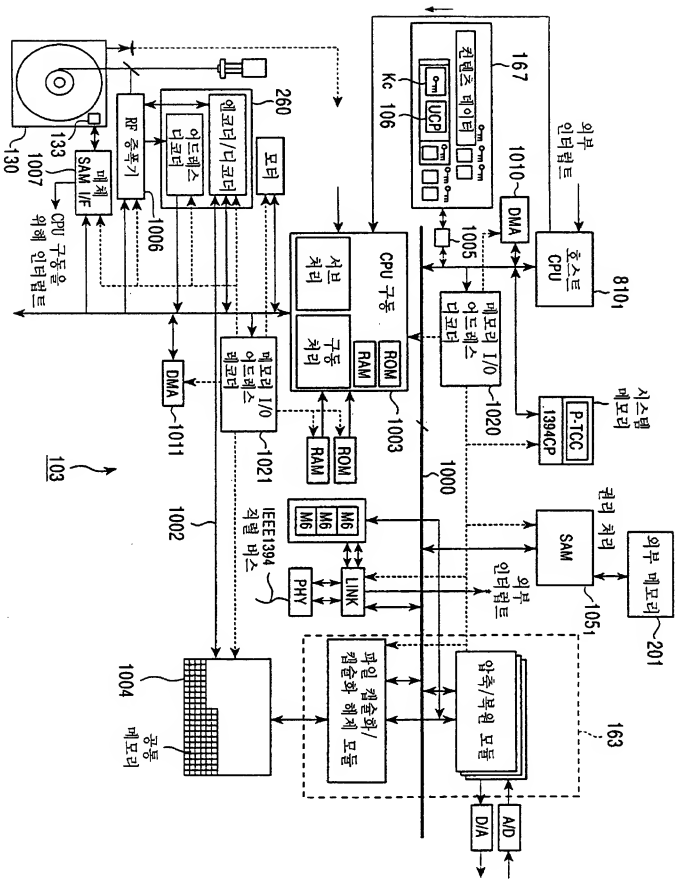


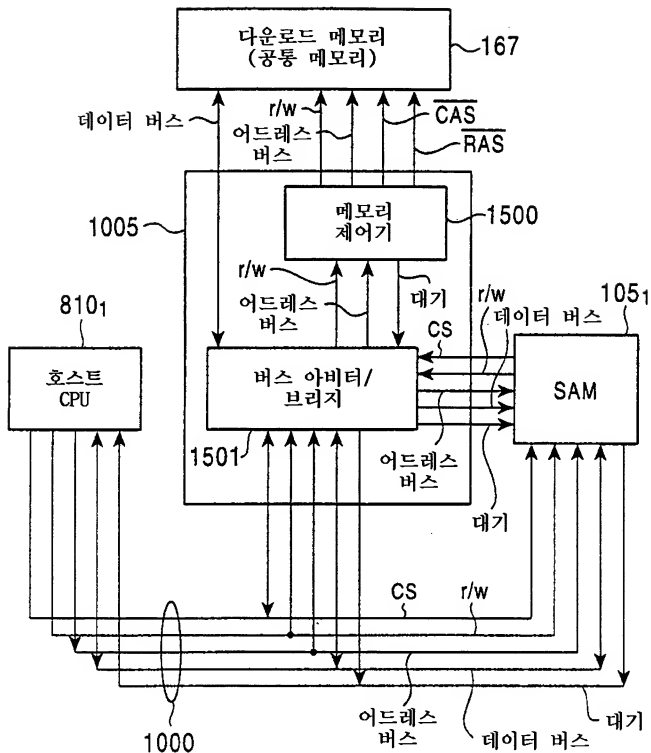
X. 509 CRL 포맷

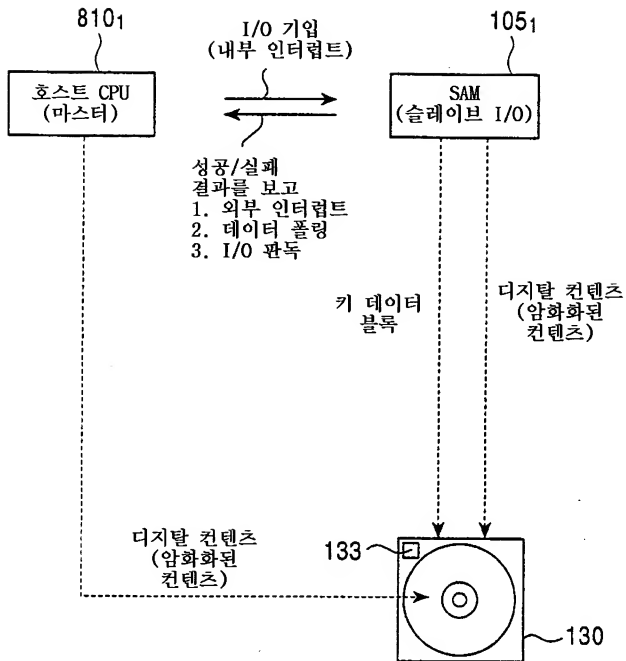


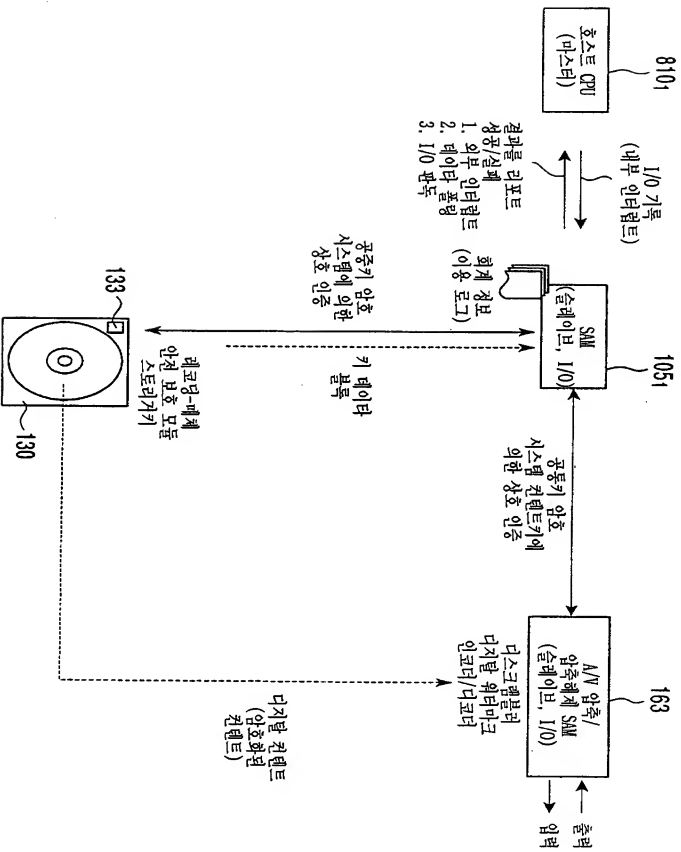


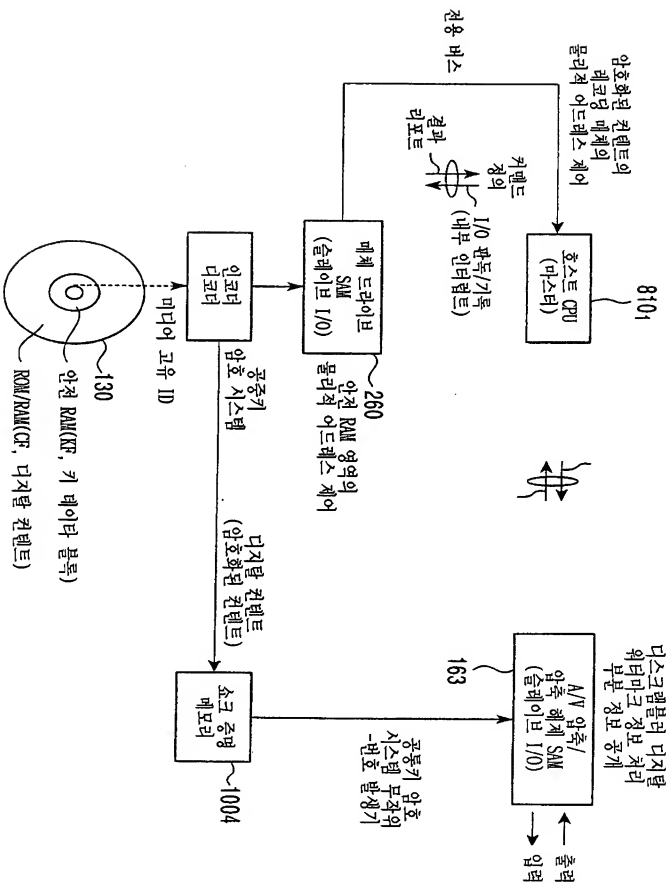


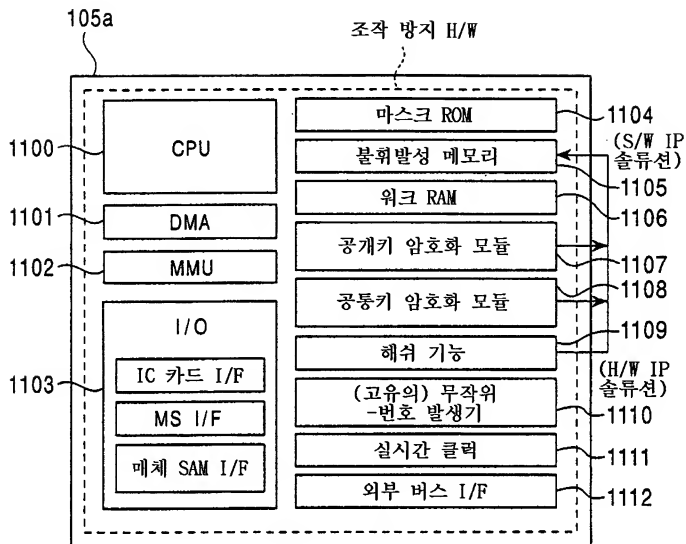


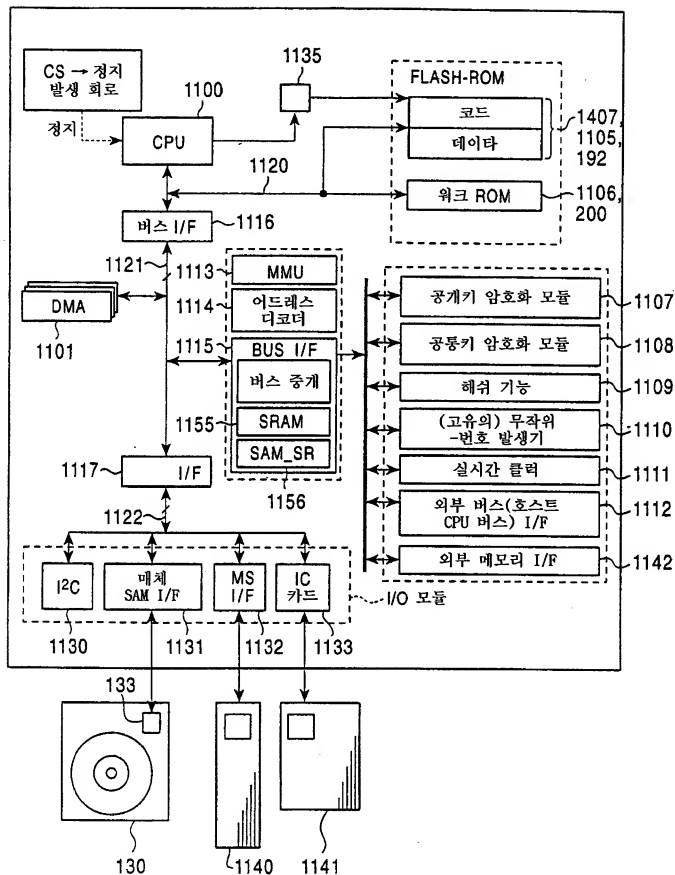


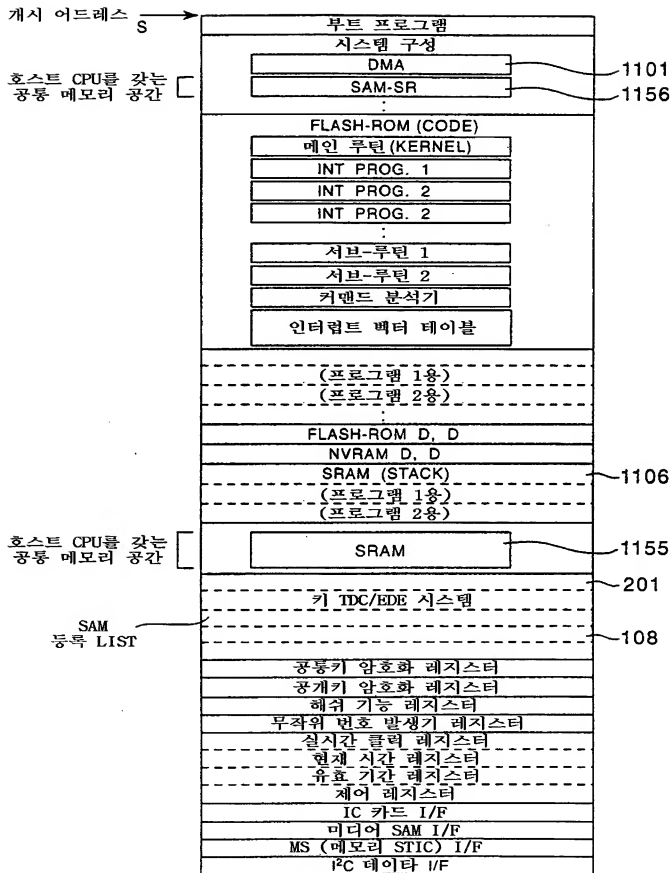


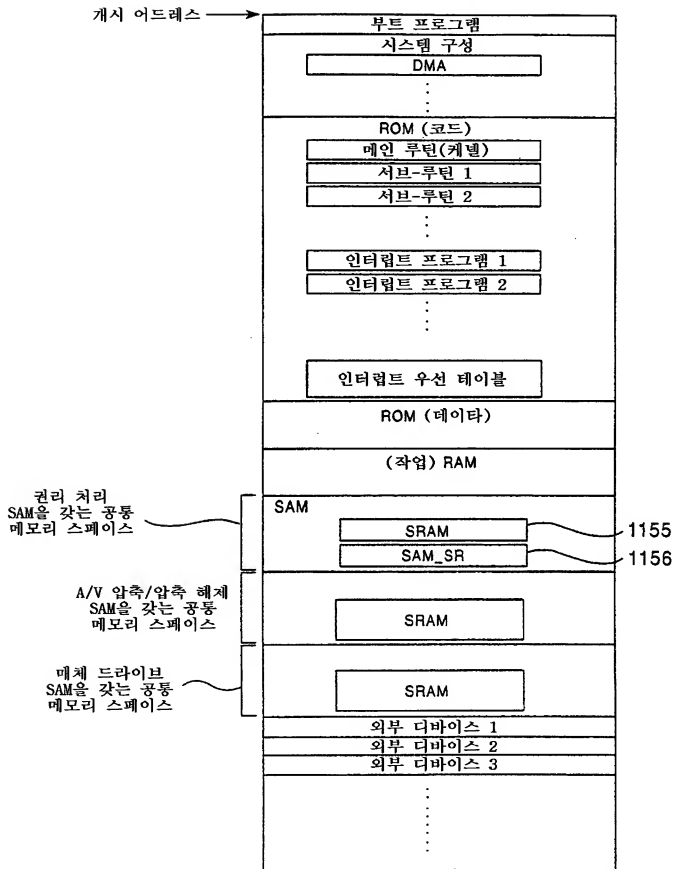


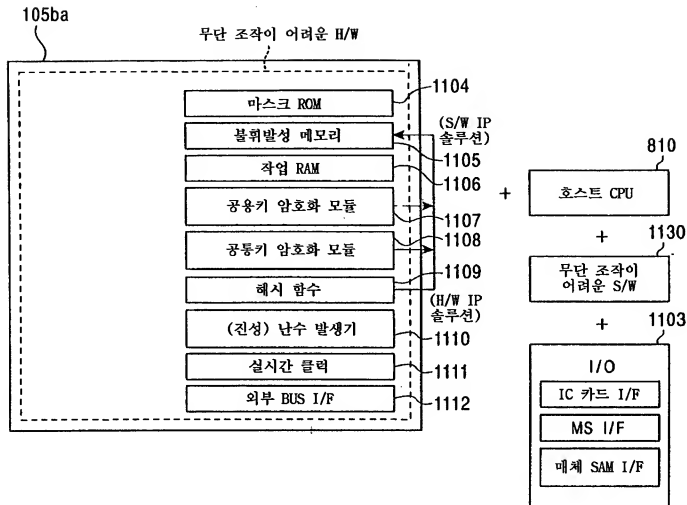


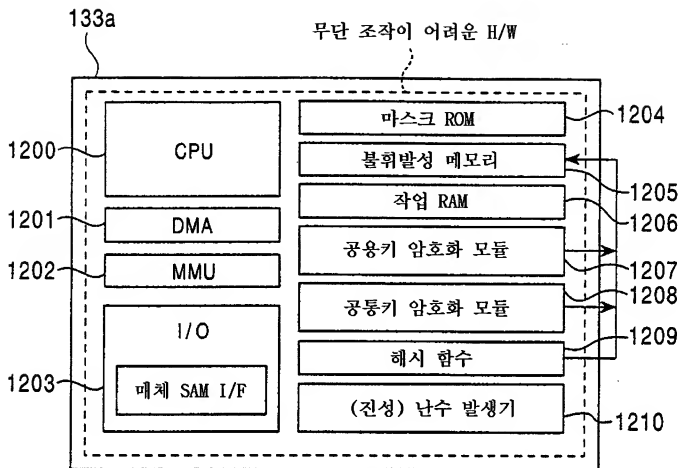












매체 SAM ID	
저장키 KSTR (매체키 KMED)	
제3자의 공용키 (EMD 서비스 센터)	
루트 CA의 공용키	
매체 SAM(X. 509)의 공용키 확인 (X.509)	
매체 SAM의 공용키 및 전용키	
취소 리스트(갱신된 값)	
이익금을 수령하는 권리 처리(이익금 분배)	
매체 유형 • 매체 유형 정보 • ROM 또는 RAM	
키 파일 KF의 물리 어드레스 정보 (레지스터 공간)	체크값
체크값(MAC)	
컨텐츠 번호 #1의 KF	체크값 (MAC)
컨텐츠 번호 #2의 KF	
컨텐츠 번호 #3의 KF	
컨텐츠 번호 #4의 KF	
컨텐츠 번호 #5의 KF	
.	
.	
컨텐츠 번호 #n의 KF	
체크값(MAC)	

허가키 KD에
의한 암호문

허가키 KD에
의한 암호문

매체 SAM ID	
저장키 KSTR (매체키 KMED)	
사용자 ID	
패스 워드	
신호 정보	
설정 정보(신용 카드 번호)	
전자 화폐	
제3자의 공개키(EMD 서비스 센터)	
루트 CA의 공용키	
매체 SAM의 공용키 확인 (X.509)	
매체 SAM의 공개키 및 전용키	
취소 리스트(갱신된 값)	
이익금을 수령하는 권리 처리(이익금 분배)	
매체 유형 • 매체 유형 정보 • ROM 또는 RAM	
키 파일 KF의 물리 어드레스 정보 (레지스터 공간)	체크값
컨텐츠 번호 #1의 KF/KF ₁	체크값 (MAC)
컨텐츠 번호 #2의 KF/KF ₁	
컨텐츠 번호 #3의 KF/KF ₁	
컨텐츠 번호 #4의 KF/KF ₁	
컨텐츠 번호 #5의 KF/KF ₁	
·	
·	
·	
컨텐츠 번호 #n의 KF/KF ₁	
체크값(MAC)	

라이선스키 KD에
의한 암호문

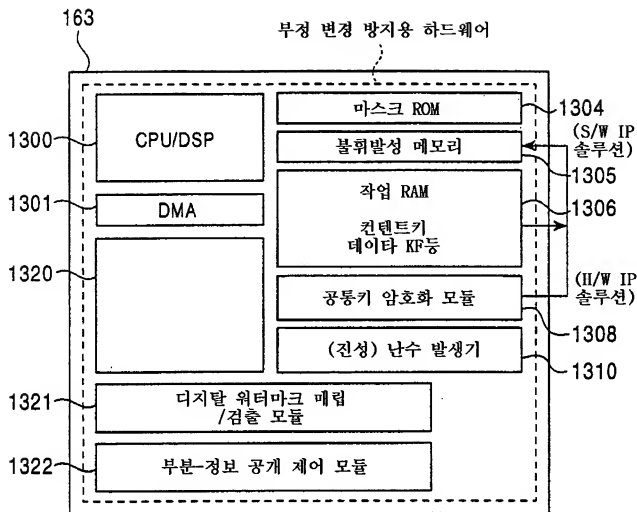
라이선스키 KD에
의한 암호문

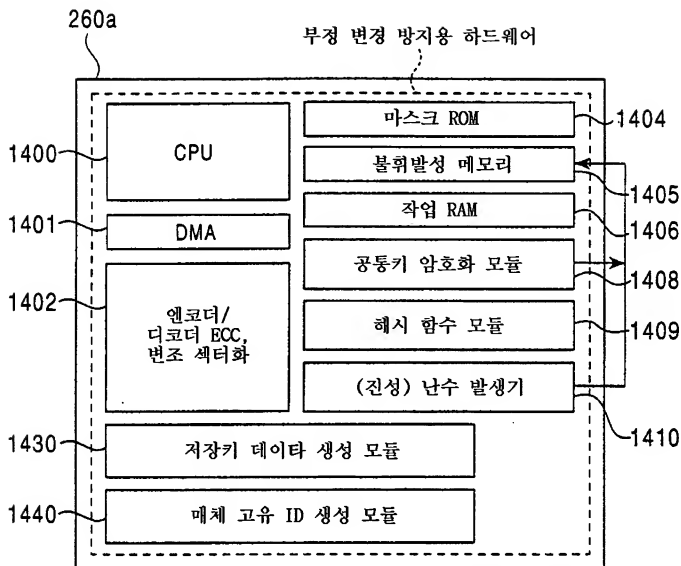
매체 SAM ID
저장키 KSTR (매체키 KMED)
제3자의 공개키(EMD 서비스 센터)
근원 CA의 공개키
매체 SAM의 공개키 증명서 (X.509)
매체 SAM의 공개키 및 비밀키
취소 리스트(갱신값)
이익금을 수령하는 소유권 처리(이익금 분배) 데이터 엔티티 ID
매체 유형 <ul style="list-style-type: none"> • 매체 유형 정보 • ROM 또는 RAM

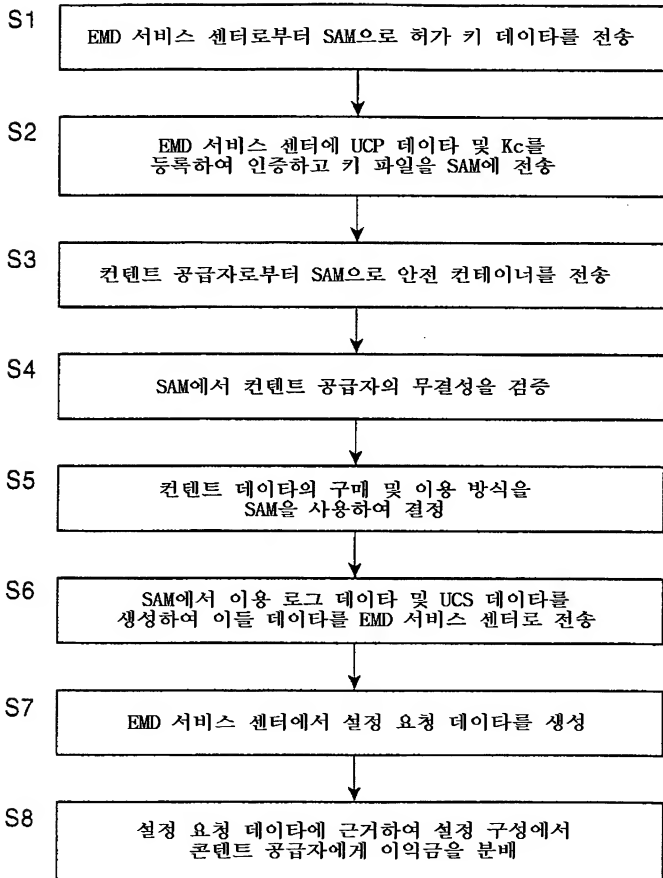
매체 SAM ID	
저장키 KSTR (매체키 KMED)	
사용자 ID	
비밀 번호	
선택 정보	
설정 정보(신용 카드 번호)	
전자 화폐	
제3자의 공개키(EMD 서비스 센터)	
근원 CA의 공개키	
매체 SAM의 공개키 증명서 (X.509)	
매체 SAM의 공개키 및 비밀키	
취소 리스트(갱신값)	
이익금을 수령하는 소유권 처리(이익금 분배) 데이터 엔터티 ID	
매체 유형 • 매체 유형 정보 • ROM 또는 RAM	
키 파일 KF의 물리 어드레스 정보 (레지스터 공간)	체크값
체크값(MAC)	
컨텐츠 번호 #1의 KF/KF _i	체크값 (MAC)
컨텐츠 번호 #2의 KF/KF _i	
컨텐츠 번호 #3의 KF/KF _i	
컨텐츠 번호 #4의 KF/KF _i	
컨텐츠 번호 #5의 KF/KF _i	
.	
.	
컨텐츠 번호 #n의 KF/KF _i	체크값(MAC)
체크값(MAC)	

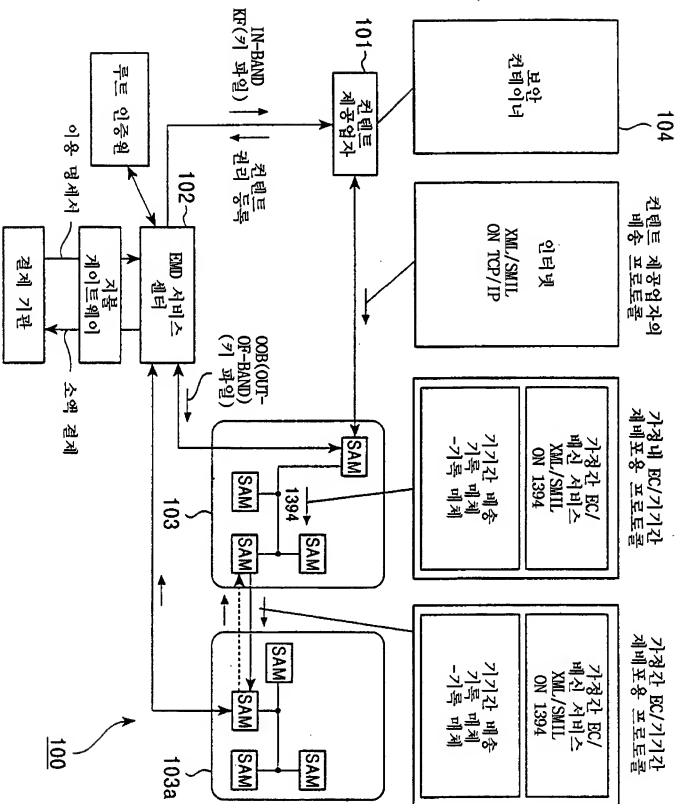
저장키 KSTR 에 의한
암호화문

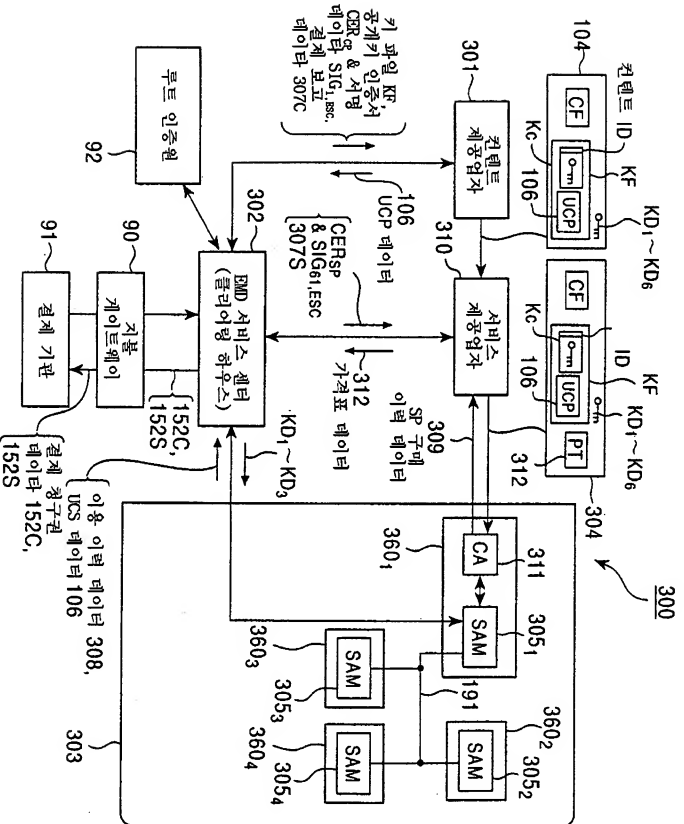
저장키 KSTR 에 의한
암호화문

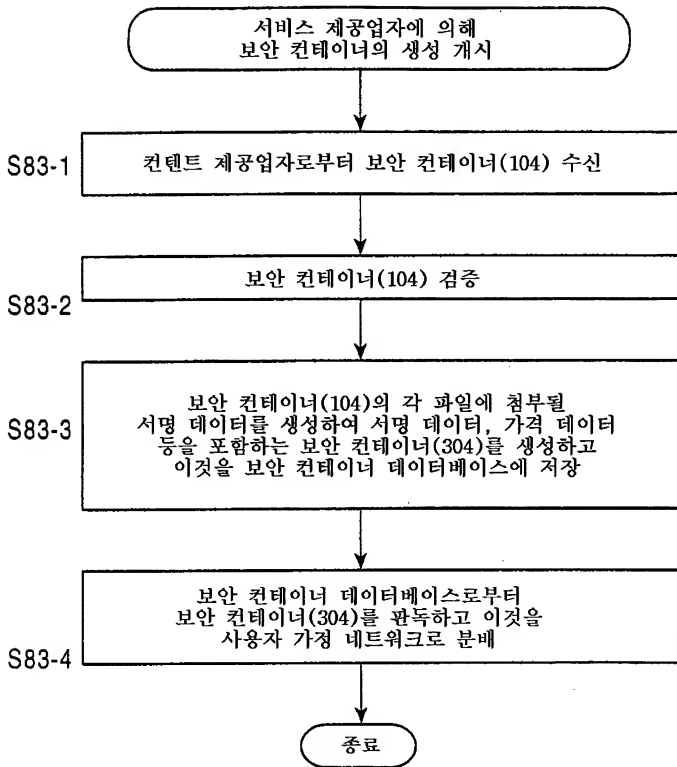


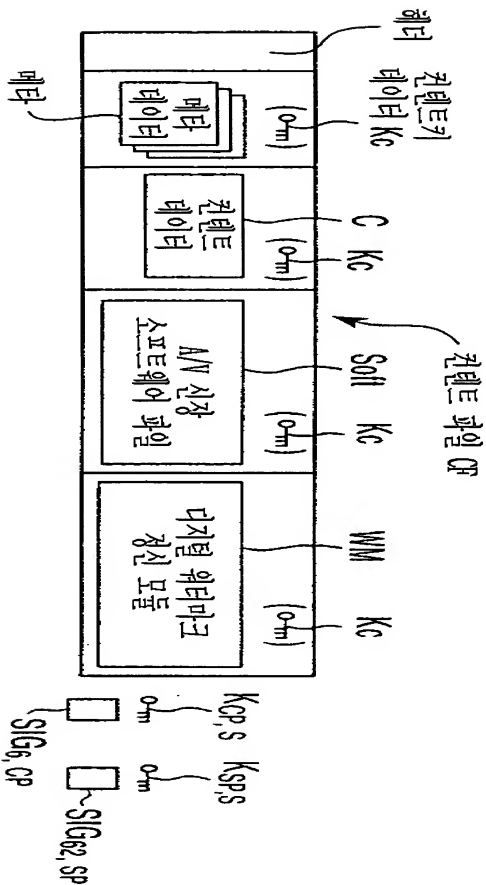


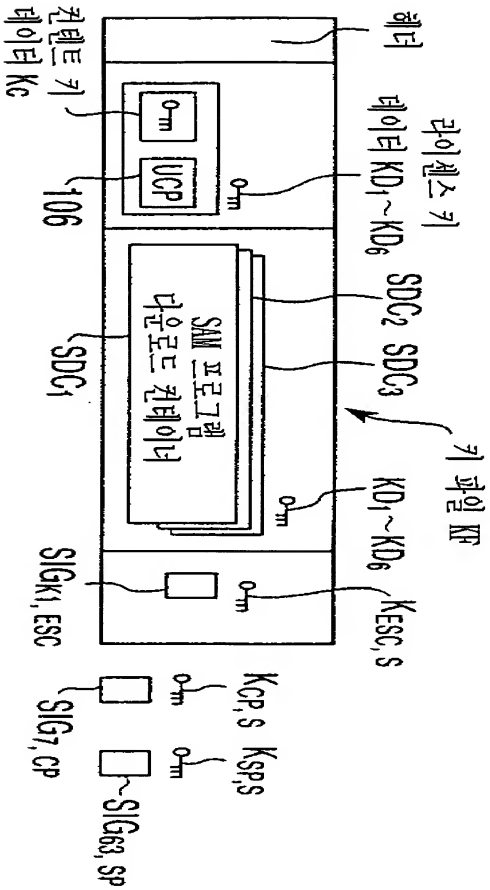


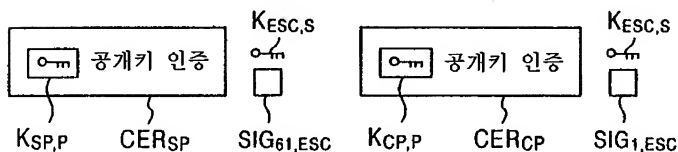
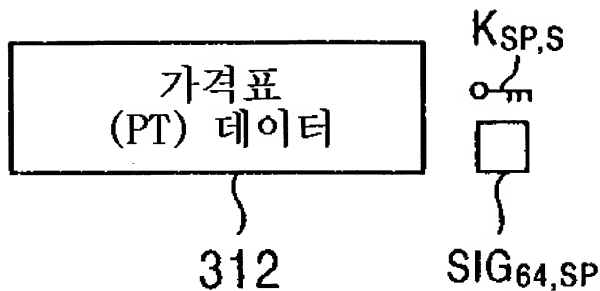


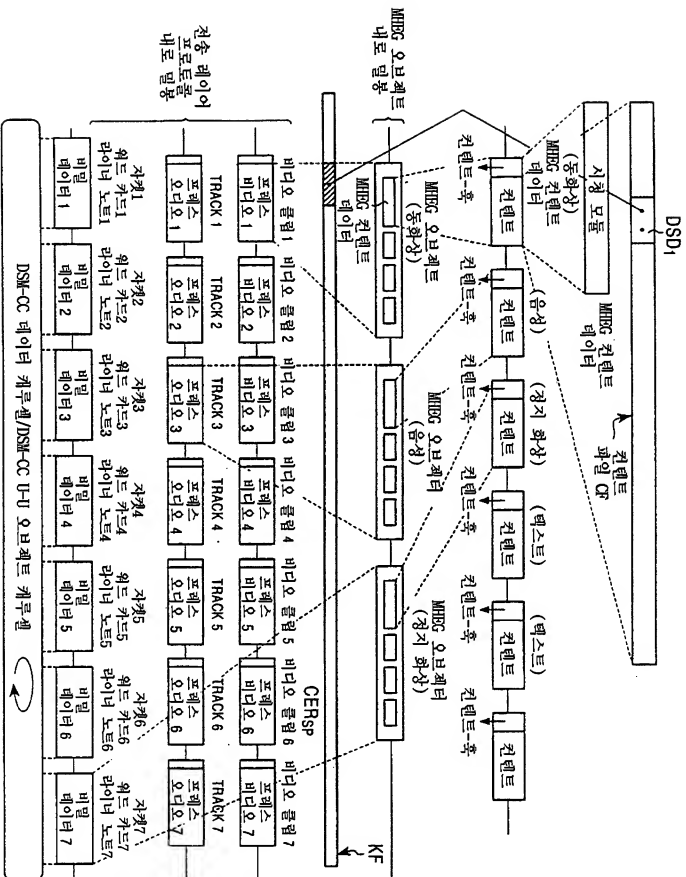


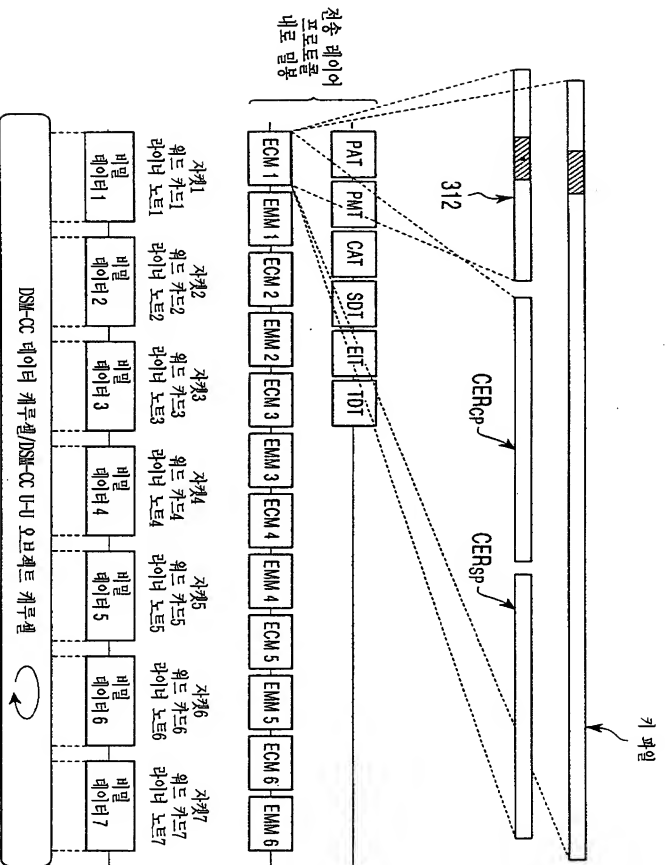










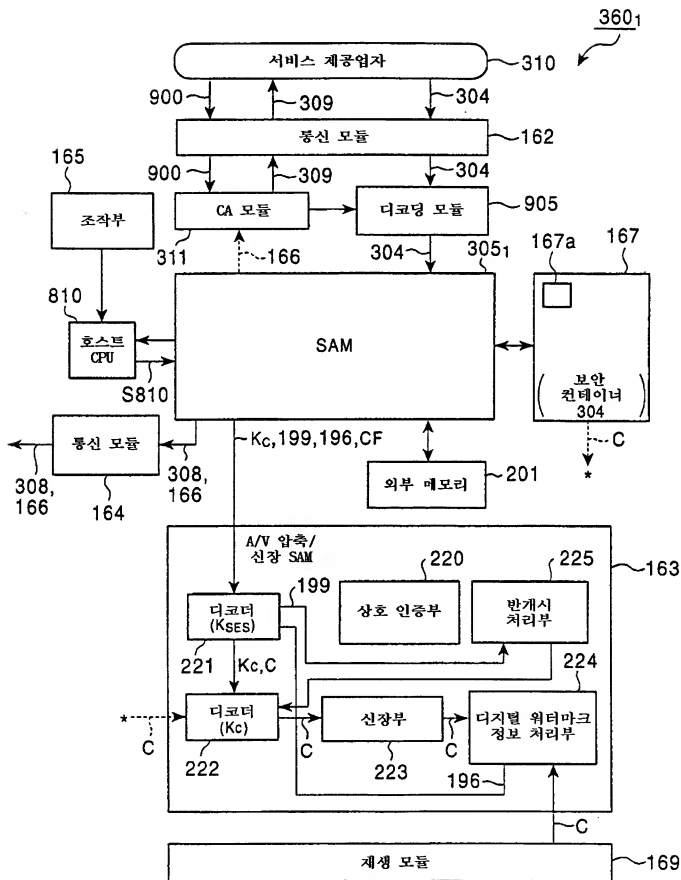


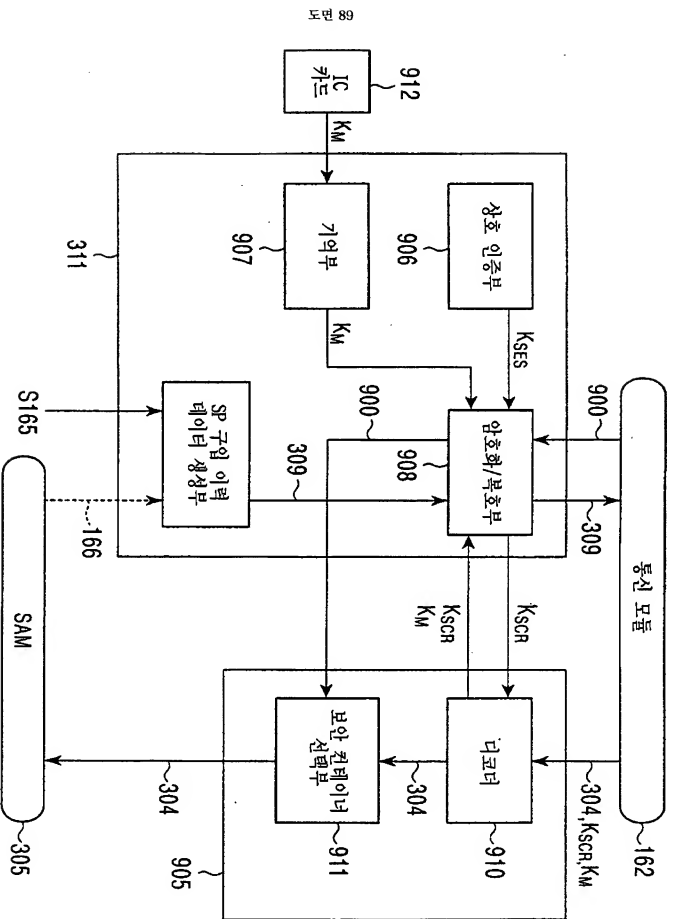
컨텐츠 제공업자 및 SAM에
라인센스키 데이터 공급

공개키 인증 데이터
DER_{CP}, CER_{SP}, CER_{SAM1} ~
CER_{SAM4}를 발행

키 파일 KF 생성

이용 기록 데이터에 따라
지불 결제 (CP와 SP 사이의
이익 분배) 처리





컨텐츠키 데이터 Kc

UCP 데이터 106

불휘발성 메모리의 로크키 데이터 201

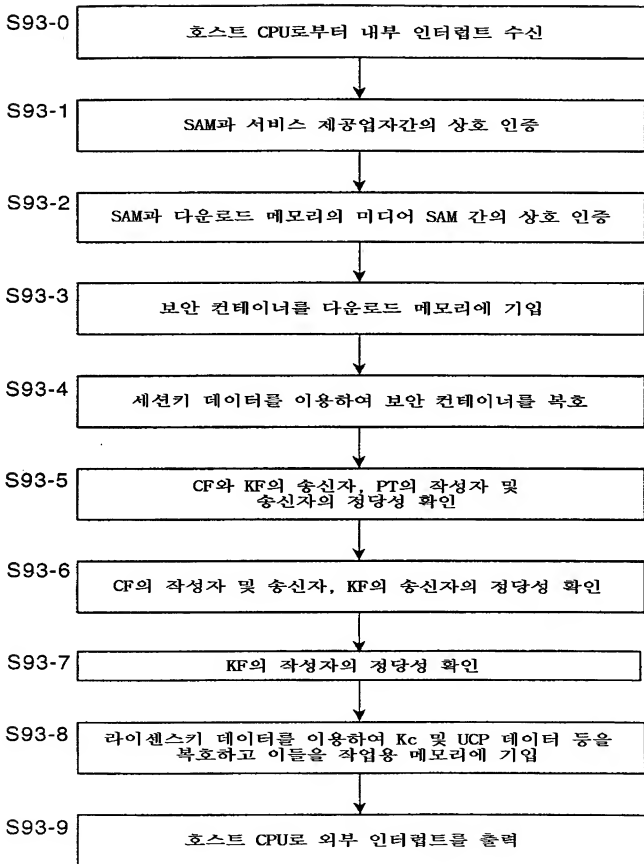
컨텐츠 제공업자의 공개키 인증 데이터 301

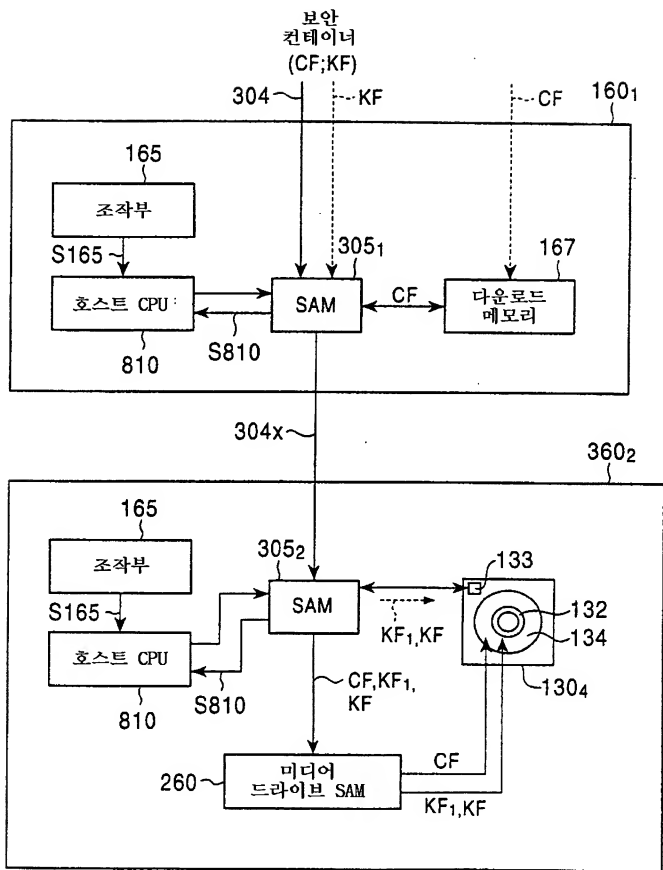
서비스 제공업자의 공개키 인증 데이터 301

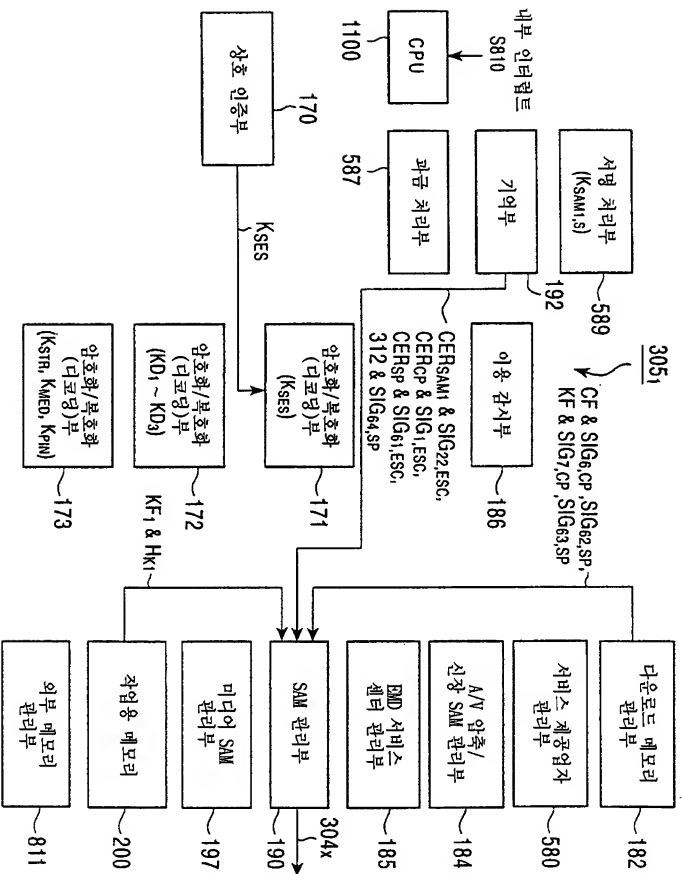
UCS 데이터 166

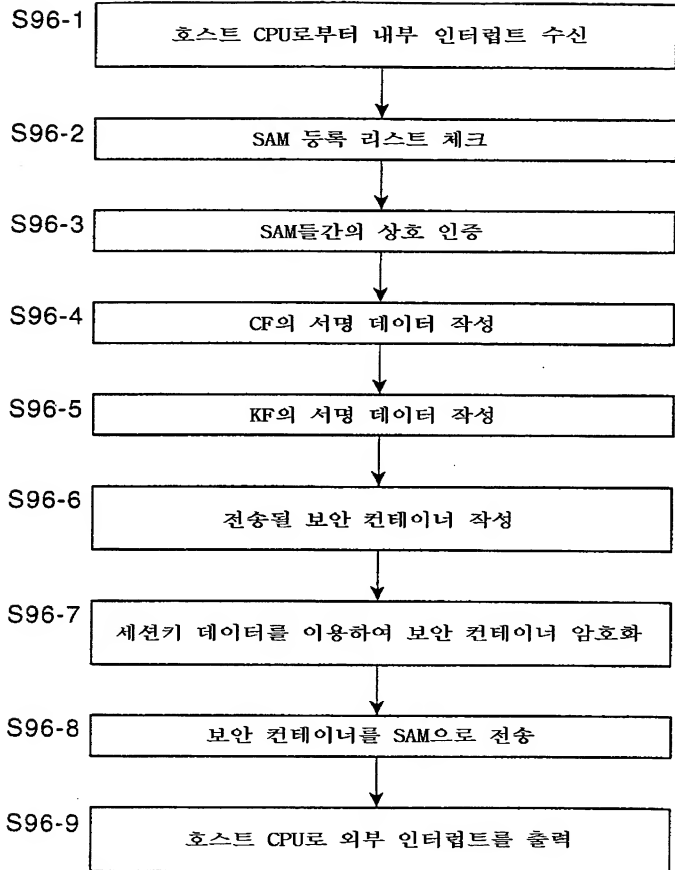
SAM 프로그램 다운로드 컨테이너

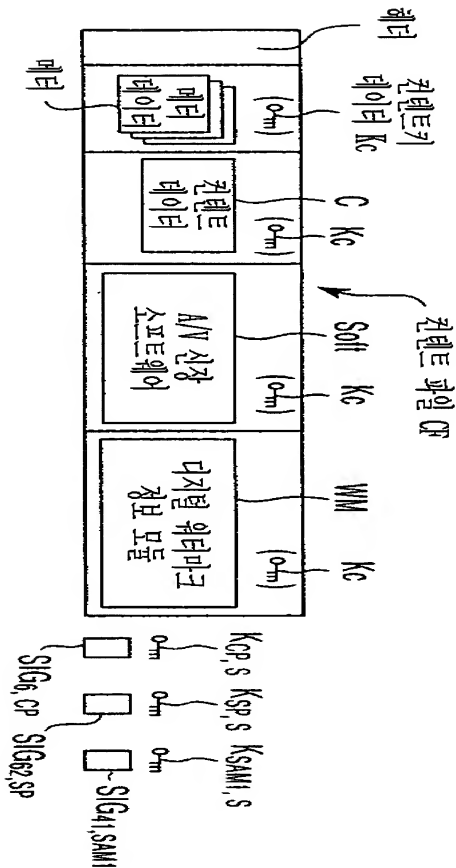
가격표 데이터 312



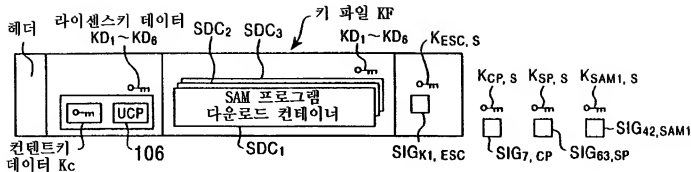




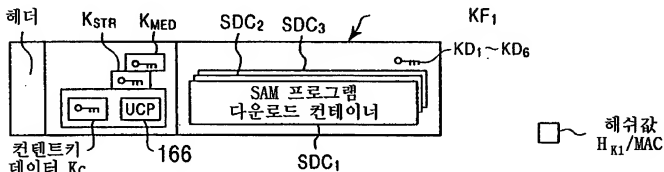




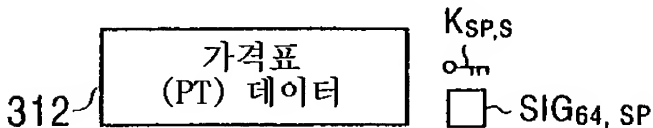
도면 97b



도면 97c



도면 97d



도면 97e

